Kryptomaskar och deras konsekvenser

Åtgärder för cybersäkerhet utifrån fallen WannaCry och NotPetya

ERIK SVENSSON, JONAS MAGNUSSON,
ERIK ZOUAVE

FOI-R--4774--SE
ISSN 1650-1942 Juni 2019

Erik Svensson, Jonas Magnusson,
Erik Zouave

Kryptomaskar och deras konsekvenser

Åtgärder för cybersäkerhet utifrån fallen WannaCry och NotPetya

Titel	Kryptomaskar och deras konsekvenser
Title	Cryptoworms and their consequences: Cybersecurity measures based on the cases WannaCry and NotPetya
Rapportnr	FOI-R--4774--SE
Månad	Juni
Utgivningsår	2019
Sidor	56 p
Kund	FOI
Forskningsområde	5. Krisberedskap och samhällssäkerhet
FoT-område	
Projektnr	I149816
Godkänd av	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Denna rapport undersöker, genom öppna svenska och engelska källor, vilka konsekvenser kryptomaskarna WannaCry och NotPetya haft för organisationer internationellt i sektorer definierade i NIS-direktivet. Rapporten undersöker varför incidenter uppstod och vilka åtgärder som drabbade organisationer och ansvariga myndigheter vidtog.

Störningar i organisationers primära tjänsteleveranser till följd av kryptomaskarna ter sig ha varit begränsade och konsekvenserna var främst ekonomiska. Inga dödsfall eller allvarliga konsekvenser för allmän säkerhet har identifierats. Främst administrativa system verkar ha drabbats. Organisationer som till hög grad var beroende av administrativa system för den primära tjänsteleveransen fick allvarligare störningar i tjänsteleveransen.

Rapporten visar att bristande cyberhygien gjort organisationer sårbara samt bidragit till kryptomaskarnas spridning, särskilt i fallet WannaCry. NotPetyas mer avancerade spridningsmekanism var svårare att förutse och förebygga, vilket ökar vikten av kontinuitetshantering. Genom alternativa arbetsrutiner hanterade vissa organisationer incidenter väl, trots störningar i IT-system. Rapporten identifierar åtgärder som höjt organisationers förmåga att förhindra och hantera kryptomaskar; åtgärder som höjer nivån av cyberhygien och kontinuitetshantering, samt förbättrar informationsdelning i incidenthantering.

Då störningarna i tjänsteleveranser stundvis var lindriga väcks frågor om liknande incidenter skulle uppfylla incidentrapporteringskrav. Kombinerat med kryptomaskars spridningshastighet väcker detta vidare frågor kring effektivt och tidigt lägesbildskapande vid utbrott av skadlig kod och påvisar vikten av informationsdelning.

Nyckelord: kryptomaskar, WannaCry, NotPetya, cybersäkerhet, cyberhygien, kontinuitetshantering, resiliens, NIS-direktivet.

Summary

This report investigates, through open English and Swedish sources, consequences of cryptoworms WannaCry and NotPetya for organisations globally in sectors defined by the NIS-directive. The report investigates why the incidents occurred and what countermeasures were implemented to manage incidents and consequences.

Primary service delivery disruptions in affected organisations seem to have been limited and consequences primarily economical. No deaths or serious threats to public safety were identified. Primarily administrative IT-system were affected. Organisations more dependent on administrative IT-systems in their primary service delivery suffered more severe disruptions.

Lacking cyber hygiene made organisations vulnerable and contributed to the spread of the cryptoworms, particularly WannaCry. NotPetya's advanced propagation mechanism made it difficult to anticipate and prevent, highlighting the need for continuity management. Some organisations handled incidents well despite disruptions in IT systems by switching to alternative routines. Identified measures to prevent and manage cryptoworms include improving the level of cyber hygiene and continuity management, as well as incident management information sharing.

As disruptions sometimes were limited, questions arise whether such incidents would trigger incident reporting requirements. Combined with the high spreading speed of cryptoworms it raises further questions about early situational awareness, highlighting the need for effective information sharing in incident management.

Keywords: cryptoworms, WannaCry, NotPetya, cyber security, cyber hygiene, continuity management, resilience, NIS-directive.

Innehållsförteckning

1 Introduktion

Under 2017 inträffade två uppmärksammade IT-angrepp: WannaCry och NotPetya. Angreppen utgjordes av kryptomaskar, det vill säga skadlig kod som krypterar offrets system och stänger av användarens tillgång till systemet.[1] WannaCry agerade som ett gisslanprogram[2] och krävde en lösensumma av användaren för att denne skulle återfå kontroll över sina system. Även om NotPetya delvis också var ett gisslanprogram, fanns inte samma möjlighet att återskapa tillgången till systemet. Gemensamt för båda kryptomaskarna är att de fick spridning i flera länder och orsakade skador i privat och offentlig verksamhet. Uppskattningsvis infekterades över 300 000 system av WannaCry[3] och NotPetya kan ha orsakat skador till ett värde av en till tio miljarder US dollar.[4] WannaCry hade en opportunistisk spridning, präglad av ekonomiska incitament. NotPetya förefaller däremot ha varit ett riktat och mer sofistikerat angrepp mot företag verksamma i Ukraina.

1.1 Syfte och frågeställningar

Denna rapport kartlägger vilka konsekvenser kryptomaskar kan ha för organisationer och vilka åtgärder som är lämpliga för att förebygga, motverka och hantera kryptomaskar. Rapporten innefattar fallstudier av kryptomaskarna WannaCry och NotPetya, vilken inverkan de hade på organisationer och hur angreppen hanterades. Rapporten utgår från definitioner tagna från Europeiska unionens (EU) direktiv om säkerhet i nätverks- och informationssystem, vanligen kallat NIS-direktivet.[5] Direktivet syftar till att höja säkerheten i nätverks- och informationssystem hos leverantörer av samhällsviktiga tjänster och rapporten syftar därför till att ge identifiera åtgärder som kan knytas till implementationen av NIS-direktivet och cybersäkerhet hos leverantörer av samhällsviktig verksamhet. Baserat på denna syftesbeskrivning besvarar rapporten två frågeställningar:

1. vilka konsekvenser ledde kryptomaskarna WannaCry och NotPetya till?
2. vad krävs för att organisationer ska kunna förebygga och hantera kryptomaskar?

1.2 Metod

NIS-direktivet listar ett antal sektorer som medlemsstaterna ska identifiera leverantörer av samhällsviktiga tjänster i: energisektorn, transportsektorn, bankverksamhetssektorn, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, distribution av dricksvatten. Utöver detta lägger rapporten till två sektorer, offentlig förvaltning och posthantering. Detta är i enlighet med NIS-direktivet som föreskriver EU:s medlemsstater rätten att själva inkludera sektorer där de anser leverantörer av samhällsviktiga tjänster finns. Dessa två sektorer har identifierats som möjliga tillägg i ett EU-meddelande om maximalt utnyttjande av direktivet.[6] Sektorerna används i rapporten för att kategorisera drabbade organisationer.

[1] Nyberg, Katinka. ”Var uppmärksammad på Ransomware”. Atrox, u.d. https://atrox.se/var-uppmarksammad-pa-ransomware/ [Hämtad: 2019-03-27].
[2] Ibid.
[3] *BBC News*. “Cyber-attack: US and UK blame North Korea for WannaCry”. 2017-12-19. https://www.bbc.com/news/world-us-canada-42407488 [Hämtad: 2019-03-27].
[4] O’Connor, Fred. ”NotPetya still roils company´s finances costing organizations $1.2 billion in revenue”. Cyberreason, 2017-11-09. https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue [Hämtad: 2019-03-27]; Greenberg, Andy. “The untold story of NotPetya, the most devastating cyberattack in history”. *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].
[5] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen EUT L 194, 19.7.2016, s. 1–30
[6] COM 2017/476: MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET: Maximalt utnyttjande av it-säkerhetsdirektivet – mot ett effektivt genomförande av direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks och informationssystem i hela unionen. Bilaga, s. 23-24.

Rapporten söker inte att befästa huruvida en drabbad organisation är en faktisk leverantör av samhällsviktiga tjänster i linje med NIS-direktivets definitioner; den kommer inte att validera om tjänsteleveransen är beroende av nätverks- och informationssystem eller om en incident i systemen har potential att uppnå NIS-direktivets tröskel för betydande störning.[7] För att kunna mäta konsekvenserna av WannaCry och NotPetya använder sig kartläggningen av NIS-direktivets måttstock för vad som ska anses vara en betydande störning. Kriterierna innefattar:

a) det antal användare som är beroende av den tjänst som den berörda entiteten[8] tillhandahåller

b) hur beroende andra sektorer definierade i direktivets bilaga II är av den tjänst som entiteten tillhandahåller

c) vilken inverkan incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet eller allmän säkerhet, uttryckt i grad och varaktighet

d) entitetens marknadsandel

e) hur stort geografiskt område som skulle kunna påverkas av en incident

f) entitetens betydelse för upprätthållandet av en tillräcklig tjänstenivå, med beaktande av tillgången till alternativa sätt för att tillhandahålla tjänsten.[9]

Även direktivets definition av vad som bör klassas som en incident används i denna studie, dvs. ”händelse med en faktisk negativ inverkan på säkerheten i nätverks- och informationssystem”,[10] mätbart bland annat genom antalet påverkade användare av tjänsten eller incidentens varaktighet.[11]

Rapporten använder sig av öppna källor från främst media för att kunna studera WannaCry och NotPetya. Inledningsvis gjordes sökningar på ”WannaCry”, ”NotPetya” och termer relevanta för de identifierade sektorerna. För att ytterligare centrera urvalet har tidsramen för incidenterna, året 2017, varit vägledande. Därefter har resultatet av artikelsökningen filtrerats efter tillgänglighet, särskilt i hänseende språk. Främst material på svenska och engelska har använts.

Då mycket av den offentliga kunskapen om angreppen är baserad på internationell medierapportering, finns det både språkliga barriärer och barriärer relaterade till källorna och dess ursprung som kan begränsa möjligheterna att ge en uttömmande bild. Delar av rapporteringen om dessa kryptomaskar har tenderat att fokusera på nyhetsvärde snarare än på detaljrikedom. Exempelvis kan det finnas mer för nyhetsbyråer att vinna på att publicera tidig, mer spekulativ (och stundvis alarmistisk)[12] rapportering, än en mer granskande text som också skulle kräva mer resurser. Materialet reflekterar ofta vad som hänt efter att en incident inträffat snarare än vad som har förebyggt en incident.

1.3 Disposition

Kapitel 2 presenterar en bakgrundsbeskrivning av WannaCry och NotPetya. Därefter i kapitel 3 presenteras även resultatet av studien av kryptomaskarnas konsekvenser. I kapitel 4

[7] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen EUT L 194, 19.7.2016, s. 1-30, artikel 6.

[8] Den svenskspråkiga versionen av direktivet använder ordet enhet som en översättning på det engelska ordet *entity*. För att särskilja mellan en teknisk enhet och vad direktivet åsyftar använder rapporten synonymen entitet.

[9] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen EUT L 194, 19.7.2016, s. 20, artikel 14.4.

[10] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen EUT L 194, 19.7.2016, s. 1–30, Artikel 4.

[11] Ibid., artikel 6.

[12] Brito, Jerry och Watkins, Tate. “Loving the cyber bomb-the dangers of threat inflation in cybersecurity policy”. *Harvard National Security Journal* 3, nr. 1 (2018): 39-84.

presenterar rapporten en analys av förutsättningarna för organisationer och ansvariga myndigheter att förebygga, bemöta och hantera kryptomaskar. Kapitel 5 presenterar rapportens slutsatser.

2 Kryptomaskarna WannaCry och NotPetya

Det finns ett flertal olika benämningar på de kryptomasker som analyseras i rapporten. Denna rapport använder **WannaCry** (även känd som *Wanna-Decryptor*[13], *WannaCrypt*[14]) och **NotPetya** (även känd som Diskcoder.c[15], ExPetr, PetrWrap, och i vissa fall felaktigt rapporterats som Petya).[16] Följande kapitel kommer efter en kort inledning beskriva respektive kryptomask, dess bakgrund och konsekvenser.

WannaCry och NotPetya har vanligen kategoriserats som gisslanprogram eller som skadlig kod som förhindrar att användaren kommer åt sina filer eller sitt system, till exempel genom att kryptera filer. Därefter utkrävs en lösensumma från användaren för att återställa filerna eller systemet. Metoden spelar ofta på användarens ovilja att förlora viktig data eller att känslig information ska röjas.[17] Genom att betala lösensumman lovas användaren återfå tillgången till sina filer.

Både NotPetya och WannaCry använder kryptering, men enbart WannaCry innefattade en fungerande lösensummafunktion. Detta skulle kunna tyda på att NotPetyas gisslanliknande konstruktion var en täckmantel för ett annat syfte.[18] WannaCry krypterade filer som var viktiga för användaren, men bibehöll systemets funktion. NotPetya krypterade även huvudstartsektorn som behövs för att kunna starta operativsystemet.[19]

Ett antal bedömare menar att NotPetya således inte är att betrakta som ett gisslanprogram utan att syftet främst var att förstöra data genom kryptering,[20] vilket i sin tur har föranlett diskussion om huruvida NotPetya var en kamouflerad cyberattack riktad mot Ukraina.[21]

Flera källor beskriver NotPetya och WannaCry utifrån spridningsmekanismer och den teknik som används för att blockera användarens tillgång till sitt system.[22] Båda beskrivs som självspridande datormaskar[23], vilket sammanfaller med att många cybersäkerhetsexperter under 2016 varnade för kryptomaskar som en ny generation av gisslanprogram. Varningen fokuserade på just den självspridande funktionen, och betonade att datormaskar med kryp-

[13] Woollaston, Victoria. "Wanna Decryptor ransomware appears to be spawning and this time it may not have a kill switch". *Wired*, 2017-05-16. https://www.wired.co.uk/article/wanna-decryptor-ransomware [Hämtad: 2019-03-27].

[14] Microsoft MSRC Team. "Customer Guidance for WannaCrypt attacks". *Microsoft TechNet*, 2017-05-12. https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ [Hämtad: 2019-03-27].

[15] Cherepanov, Anton. "TeleBots are back: Supply-chain attacks against Ukraine. *We Live Security*, 2017-06-30. https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/ [Hämtad: 2019-03-27].

[16] Ibid.

[17] Al-Rimy, B.A.S., Maarof, M.A. och Shaid, S.Z.M. "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions", *Computers & Security* 74 (2018), s. 144-166.

[18] Shepherd, Adam. "NotPetya was nastier than WannaCry ransomware, say experts". *IT Pro*, 2017-11-01. http://www.itpro.co.uk/security/29863/notpetya-was-nastier-than-wannacry-ransomware-say-experts [Hämtad: 2019-03-27].

[19] Fruhlinger, Josh. "Petya ransomware and NotPetya malware: What you need to know now". *CSO Online*, 2017-10-17. https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html [Hämtad: 2019-03-27].

[20] Duckett, Chris. "Ransomware in disguise: Experts say Petya out to destroy not ransom". *ZDNet*, 2917-06-29. https://www.zdnet.com/article/ransomware-in-disguise-experts-say-petya-out-to-destroy-not-ransom/ [Hämtad: 2019-03-27].

[21] Fruhlinger, Josh. "The 5 biggest ransomware attacks of the last 5 years". *CSO Online*, 2017-08-01. https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html [Hämtad: 2019-03-27].

[22] Hern, Alex. "WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017". *The Guardian*, 2017-12-30. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware [Hämtad: 2019-03-27].

[23] Rice, Adam. "Why WannaCry and other computer worms may inherit the earth". *SearchSecurity*, 2017-09-01. https://searchsecurity.techtarget.com/feature/Why-WannaCry-and-other-computer-worms-may-inherit-the-earth [Hämtad: 2019-03-27].

tografisk låsningsfunktion på ett autonomt sätt skulle kunna uppnå betydligt större spridning än tidigare kända skadeprogram.[24] NotPetya och WannaCry skulle kunna ses som exempel på en sådan trend.

2.1 WannaCry

Den 12 maj 2017 inleddes spridningen av det gisslanprogram som sedermera fick namnet WannaCry. Två dagar senare, den 14 maj, uppgavs att över 200 000 system i 150 olika länder hade infekterats.[25] Den 17 maj uppskattades att mer än 100 000 verksamheter hade drabbats av WannaCry[26] och att siffran för antal drabbade system växt till fler än 300 000.[27]

Flera källor pekar på att WannaCrys spreds via automatisk scanning efter sårbara system.[28] Utöver system på det interna nätverket försökte WannaCry sprida sig vidare till andra nätverk. WannaCry skilde sig från tidigare gisslanprogram eftersom det inte bara försökte kryptera filer från den smittade datorn, utan också använde en sårbarhet för att sprida sig vidare i det interna nätverket. Detta ledde dels till att angriparen inte behövde skicka ut lika många mail för att sprida den skadliga koden, dels till att spridningen gick snabbare när WannaCry etablerat ett fotfäste i ett nätverk.[29] En funktion i WannaCrys kod gjorde ett kontrollanrop till en påhittad domän (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com). Om funktionen fick svar från denna domän avbröts WannaCrys körning. Genom att registrera domännamnet kunde WannaCrys spridning avbrytas.[30] Genom att spåra anslutningarna till domänen kunde spridningshastigheten uppmätas till tusentals system per sekund.[31]

När WannaCry tagit sig in i ett system, krypterades användarens filer. Ett meddelande, som täckte hela skärmen, angav att användarens alla filer krypterats. Enligt meddelandet behövde användaren betala en lösensumma i kryptovalutan Bitcoin, till ett värde av 300 US dollar, för att låsa upp filerna.[32] Redan i mars 2017 släppte Microsoft en säkerhetsupp-

[24] Storm, Darlene. ”Cryptoworms: The future of ransomware hell”. *ComputerWorld*, 2016-04-13. https://www.computerworld.com/article/3055488/security/cryptoworms-the-future-of-ransomware-hell.html [Hämtad: 2019-03-27].

[25] Piper, Elizabeth och Heinrich, Mark. “Cyber attack hits 200,000 in at least 150 countries: Europol. *Reuters*, 2017-05-14. https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX [Hämtad: 2019-03-27].

[26] Fulbright, Norton Rose. “WannaCry Ransomware Attack Summary”. *Data Protection Report*, 2017-05-17. https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/ [Hämtad: 2019-03-27].

[27] *Reuters*. ”Cyber-attack: US and UK blame North Korea for WannaCry. 2017-12-19. https://www.bbc.com/news/world-us-canada-42407488 [Hämtad: 2019-03-27].

[28] ENISA. ”WannaCry Ransomware Outburst”. 2017-05-15. https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst [Hämtad: 2019-03-27]; McNeil, Adam. “How did the WannaCry ransomworm spread?”. *Malwarebytes Labs*, 2017-05-19. https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/ [Hämtad: 2019-03-27].

[29] McNeil, Adam. “How did the WannaCry ransomworm spread?”. *Malwarebytes Labs*, 2017-05-19. https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/ [Hämtad: 2019-03-27].

[30] D’Souza-Wiltshire, Iaan; Schonning, Nick; Mackenzie, Duncan; Hall, Justin. “WannaCrypt Ransomware worm targets out-of-date systems”. Windows IT Pro Center, 2017-07-27. https://docs.microsoft.com/en-us/windows/security/threat-protection/wannacrypt-ransomware-worm-targets-out-of-date-systems-wdsi [Hämtad: 2019-03-27].

[31] Kohmami, Nadia och Solon, Olivia. ”’Accidental hero’ halts ransomware attack and warns: this is not over”. *The Guardian*, 2017-05-13. https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack [Hämtad: 2019-03-27]; Kryptos Logic. ”WannaCry: Two Weeks and 16 Million Averted Ransoms Later”. 2017-05-29. https://blog.kryptoslogic.com/malware/2017/05/29/two-weeks-later.html [Hämtad: 2019-03-27].

[32] Greenberg, Andy. “The WannaCry ransomware hackers made some real amateur mistakes”. *Wired*, 2017-05-15. https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/ [Hämtad: 2019-03-27].

datering som åtgärdade den bugg i Service Message Block-protokollet som WannaCry utnyttjade för att sprida sig vidare automatiskt till nya system.[33] Först i samband med den utbredda spridningen av WannaCry, gav Microsoft även ut en uppdatering för Windows XP.[34]

Det finns ett flertal källor som kopplar ihop WannaCry-attacken och hackergruppen Lazarus.[35] Det spekuleras i att det var gruppen som iscensatte attacken, att någon tog inspiration från gruppen eller att attackeraren hade tillgång till Lazarus verktyg.[36] FBI pekade ut en nordkoreansk hacker med kopplingar till den Nordkoreanska regimen vid namn Park Jin Hyok som kopplad till Lazarus och inblandad i WannaCry-attacken.[37] Attribution av cyberattacker är dock mycket svårt och det är därför omöjligt att med säkerhet uttala sig om huruvida Lazarus var ansvariga för attacken eller ens om gruppen överhuvudtaget har kopplingar till Nordkorea.[38]

2.2 Petya och NotPetya

I maj 2016 upptäcktes den första versionen av den skadliga mjukvara som senare fick namnet Petya. Petya spreds genom infekterade dokument bifogade i mejl. När mottagaren öppnade den bifogade filen, bad Windows om administratörsrättigheter för att göra ändringar i systemet. Om användaren godkände ändringarna, skrev Petya över huvudstartsektorn (MBR) på hårddisken samt krypterade mästerfiltabellen (MFT) som innehåller informationen om var alla andra filer finns. Därmed förlorar användaren och systemet tillgång till filerna. Likt WannaCry avkrävdes därefter användaren en lösensumma betalad i Bitcoin för att återställa tillgång till systemet.[39]

Den 27 juni 2017 rapporterades vad som antogs vara ett nytt utbrott av Petya. Det visade sig dock vara ett angrepp inom ”Petya-familjen” av gisslanprogram, och fick namnet NotPetya.[40] Petya och NotPetya uppvisade många likheter.[41] En stor skillnad var dock att NotPetya var en mask som kunde sprida sig självt mellan system. Både WannaCry och NotPetya använde sig av sårbarheten EternalBlue som utnyttjade en svaghet i version 1 av nätverksprotokollet Service Message Block.

[33] D’Souza-Wiltshire, Iaan; Schonning, Nick; Mackenzie, Duncan; Hall, Justin. “WannaCrypt Ransomware worm targets out-of-date systems”. Windows IT Pro Center, 2017-07-27. https://docs.microsoft.com/en-us/windows/security/threat-protection/wannacrypt-ransomware-worm-targets-out-of-date-systems-wdsi [Hämtad: 2019-03-27].

[34] Warren, Tom. ”Microsoft issues ’highly unusual’ Windows XP patch to prevent massive ransomware attack”. *The Verge*, 2017-05-13. https://www.theverge.com/2017/5/13/15635006/microsoft-windows-xp-security-patch-wannacry-ransomware-attack [Hämtad: 2019-03-27].

[35] Kryptos Logic. ”WannaCry: Two Weeks and 16 Million Averted Ransoms Later”. 2017-05-29. https://blog.kryptoslogic.com/malware/2017/05/29/two-weeks-later.html [Hämtad: 2019-03-27].

[36] Heller, Michael. ”Lazarus Group hacker charged in WannaCry, Sony atacks”. SearchSecurity , 2018-11-07. https://searchsecurity.techtarget.com/news/252448325/Lazarus-Group-hacker-charged-in-Wannacry-Sony-attacks [Hämtad: 2019-03-27].

[37] “PARK JIN HYOK”. FBI. 2018-08-30. https://www.fbi.gov/wanted/cyber/park-jin-hyok [Hämtad: 2019-03-27].

[38] Kaste, Martin. ”From Kill Switch To Bitcoin, ’WannaCry’ Showing Signs Of Amateur Flaws”. *National Public Radio* [webbsida], 2017-05-16. https://www.npr.org/sections/alltechconsidered/2017/05/16/528570788/from-kill-switch-to-bitcoin-wannacry-showing-signs-of-amateur-flaws?t=1537969494161 [Hämtad: 2019-03-27].

[39] Kubovič, Ondrej. ”Ransomware is everywhere, but even black hats make mistakes”. *We Live Security*, 2016-04-28. https://www.welivesecurity.com/2016/04/28/ransomware-is-everywhere-but-even-black-hats-make-mistakes/ [Hämtad: 2019-03-27]; Fruhlinger, Josh. ”Petya ransomware and NotPetya malware: What you need to know now”. *CSO Online*, 2017-10-17. https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html [Hämtad: 2019-03-27].

[40] *We Live Security*. “New WannaCryptor-like ransomware attack hits globally: All you need to know”. 2017-06-27. https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/ [Hämtad: 2019-03-27].

[41] Alvarez, Raul. ”Key Differences Between Petya and NotPetya”. *Fortinet*, 2017-07-09. https://www.fortinet.com/blog/threat-research/key-differences-between-petya-and-notpetya.html [Hämtad: 2019-03-27].

NotPetya kunde dessutom samla in inloggningsuppgifter som använts på det infekterade systemet och använda dem för att sprida sig vidare till andra system i samma nätverk. [42] NotPetya kunde således först infektera system som saknade den nödvändiga Windowsuppdateringen och sedan sprida sig vidare till system som var uppdaterade.[43] Säkerhetsföretaget Cisco menade att NotPetya var den mest snabbspridda skadliga mjukvaran företaget sett.[44]

Även NotPetya avkrävde användaren en lösensumma på 300 USD i Bitcoin för dekryptering. En aspekt som dock särskiljer NotPetya från WannaCry var att den krypteringsnyckel som användes inte sparades och användaren därför inte kunde få sitt system dekrypterat även om de betalade. Av denna anledning menar vissa att NotPetya inte är ett gisslanprogram, utan att det krypterar data med syfte att förstöra tillgången till systemet.[45] Detta förmodade syfte styrks av att NotPetya permanent skriver över de första 18 blocken på hårddisken, för att på så sätt förhindra hårddiskens funktion. Vid infektion av Petya gick liknande förändringar att återställa.[46]

NotPetya-angreppet verkar ha skett genom ett inledande angrepp riktat mot det ukrainska företaget Intellect Services servrar.[47] Företaget tillhandahåller redovisningsmjukvaran M.E.Doc, som användes av cirka 90 procent av det ukrainska näringslivet.[48] Genom detta intrång kunde skadlig kod, som bland annat inkluderade en avancerad bakdörr, placeras i företagets mjukvara. När kunderna uppdaterade sin version av M.E.Doc fick de med bakdörren, varpå angriparna fick åtkomst till deras IT-miljö för vidare angrepp.[49] Den skadliga koden återfanns dock inte i alla uppdateringar därefter. Detta har föranlett misstankar om att angriparna tidvis tappat åtkomst till Intellect Services-servrar samt att det slutgiltiga intrånget skedde tidigare än planerat, möjligtvis på grund av en rädsla att tappa tillgången permanent.[50]

Genom att använda samma kommunikationsväg som legitima M.E.Doc-uppdateringar kunde bakdörren användas för att skicka tillbaka systeminformation utan att detta flaggades som illegitim nätverks-kommunikation. Enligt IT-säkerhetsföretaget ESET kunde bakdörren användas för att skicka både skadlig kod och kommandon för att styra den. Den fungerade därför som ett verktyg för både cyberspionage och cybersabotage. [51]

Till skillnad från WannaCry fanns inget enkelt sätt att förhindra fortsatta infektioner. Däremot kunde en viss fil (C:\Windows\perfc.dat) blockeras från att skrivas av NotPetya, och

[42] Fruhlinger, Josh. ”Petya ransomware and NotPetya malware: What you need to know now”. *CSO Online*, 2017-10-17. https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html [Hämtad: 2019-03-27].

[43] Greenberg, Andy. “The untold story of NotPetya, the most devastating cyberattack in history”. *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

[44] Ibid.

[45] Ivanonov, Anton och Mamedov, Orkhan. ”ExPetr/Petya/NotPetya is a Wiper, Nor Ransomware”. *SecureList*, 2017-06-28. https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ [Hämtad: 2019-03-26]

[46] Suiche, Matt. ”Petya.2017 is a wiper not a ransomware”. *Comae Technologies* [blogg], 2017-06-28. https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b. [Hämtad: 2019-04-08].

[47] Maynor, David; Nikolic, Aleksandar; Olney, Matt och Younan, Yves. ”The M.E.Doc Connection”. *Talo Intelligence*, 2017-07-05. https://blog.talosintelligence.com/2017/07/the-M.E.Doc-connection.html [Hämtad: 2019-03-26].

[48] Borys, Christian. “Ukraine braces for further cyber-attacks”. *BBC*, 2017-07-27. https://www.bbc.com/news/technology-40706093 [Hämtad: 2019-03-26].

[49] Cherepanov, Anton. “Analysis of TeleBots’ cunning backdoor”. *ESET We Live Security*, 2017-07-04. https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ [Hämtad: 2019-03-26].

[50] Cherepanov, Anton. “Analysis of TeleBots’ cunning backdoor”. *ESET We Live Security*, 2017-07-04. https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ [Hämtad: 2019-03-26].

[51] Ibid.

därmed begränsa ett pågående angrepp. Denna åtgärd fungerade som ett vaccin som förhindrade vidare spridning globalt.[52] Det var också möjligt att i förebyggande syfte begränsa NotPetyas spridning mellan system genom att stänga av fildelning via version 1 av SMB-protokollet, blockera extern tillgång till portar 137, 138, 139, och 445, samt begränsa administratörsprivilegier.[53]

Enligt ESET fanns kopplingar mellan NotPetya och hackergruppen Telebots,[54] vilka 2015 orsakade störningar i Ukrainas elnät. Kopplingarna baserades på likheter i de verktyg som användes i attackerna, snarare än på konkreta bevis. ESET menade att Telebots även tidigare använt gisslanprogram i andra syften än att utvinna lösensummor. Kaspersky Lab, ett annat IT-säkerhetsföretag, menade också att det fanns likheter i koden men att det inte nödvändigtvis behövde indikera samma skapare. IT-säkerhetsföretaget FireEye menar att Telebots (som FireEye kallar Sandworm) har kopplingar till den ryska staten.[55]

Ukrainas råd för nationell säkerhet och försvar (National Security and Defense Council of Ukraine) och Ukrainas säkerhetstjänst SBU hävdade att Ryssland låg bakom attacken;[56] en anklagelse som baserades på att programvaran verkade ha varit en täckmantel för att skapa störningar snarare än att generera pengar.[57] Nato gav efter attacken fortsatt stöd till att stärka Ukrainas cyberförsvar.[58] I november 2017 drog CIA i en hemligstämplad rapport slutsatsen att det med hög sannolikhet var ryska GRU som skapat NotPetya.[59] Enligt CIA arbetade personerna bakom NotPetya för GTsST (”Huvudcentret för Speciell Teknologi”), en del av GRU som bedriver offensiva cyberoperationer.[60] I februari 2018 riktade Vita husets pressekreterare officiella anklagelser mot Ryssland och hävdade att Ryssland utfört NotPetya-attacken som en del av ryska destabiliseringsåtgärder riktade mot Ukraina. Det är värt att notera att inga konkreta bevis presenterades.[61]

---

[52] Bisson, David. ”NotPetya: Timeline of a Ransomworm”. *Tripwire The State of Security* [blogg], 2017-07-28. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/ [Hämtad: 2019-03-26].

[53] Thomson, Iain. “Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide”. *The Register*, 2017-06-28. https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/ [Hämtad: 2019-03-26].

[54] Brewster, Thomas. “NotPetya Ransomware Hackers ‘Took Down Ukraine Power Grid”. *Forbes*, 2017-07-03. https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/#c5e18886b89d [Hämtad: 2019-03-26].

[55] Ibid.

[56] Crosby, Alan. “Ukraine Is ‘Ground Zero’ For Hackers In Global Cyberattacks”. *Radio Free Europe Radio Liberty*, 2017-06-28. https://www.rferl.org/a/ukraine-petya-ransomware-cyberattack-ground-zero/28583931.html [Hämtad: 2019-03-26]; Polityuk, Pavel. ”Ukraine points finger at Russian security services in recent cyber attack”. *Reuters*, 2017-07-01. https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P [Hämtad: 2019-03-26].

[57] Polityuk, Pavel. ”Ukraine points finger at Russian security services in recent cyber attack”. *Reuters*, 2017-07-01. https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P [Hämtad: 2019-03-26].

[58] *Ukrinform*. ”Stoltenberg: NATO to increase aid to Ukraine in field of cyber defense”. 2017-06-28. https://www.ukrinform.net/rubric-defense/2255739-stoltenberg-nato-to-increase-aid-to-ukraine-in-field-of-cyber-defense.html [Hämtad: 2019-03-26].

[59] Nakashima, Ellen. ”Russian military was behind ‘NotPetya’ attack in Ukraine, CIA concludes”. *Washington Post*, 2018-01-02. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html [Hämtad: 2019-03-26].

[60] Ibid.

[61] “Statement from the Press Secretary”. White House, 2018-02-15. https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ [Hämtad: 2019-03-26].

3 Konsekvenser

Detta kapitel granskar av vilka konsekvenser kryptomaskarna internationellt haft på verksamhet inom energisektorn, transportsektorn, bankverksamhetssektorn, finansmarknadens infrastruktur, hälso- och sjukvårdssektorn och leverans av dricksvatten (och de i denna studie tillagda sektorerna offentlig förvaltning och posthantering).[62] Kapitlet syftar till att ge en bild av incidenter och dess konsekvenser, snarare än en kvantitativ redogörelse för alla inträffade incidenter och drabbade sektorer.

Utifrån detta identifierar rapporten en sektorsövergripande spridning av både WannaCry och NotPetya i ett flertal länder. WannaCry påverkade aktörer inom direktivets sektorer även utanför EU:s gränser och därför kommer exempel från Indien, Kina, Ryssland och USA att adderas till EU-medlemsstaterna Spanien, Sverige, Tyskland, och Storbritannien. NotPetya påverkade främst Ukraina och därför kommer fokus främst att vara på hur Ukraina drabbades och agerade.

Det är inte möjligt att i alla fall belägga exempelvis hur många användare som påverkats, vilka de sektorsövergripande beroendena varit eller vilken marknadsandel den påverkade enheten haft.

Tabell 1. Översikt över redovisade incidenter.

Sektorer	WannaCry	NotPetya
Sektorer i direktivet		
Energisektor	Indien, Spanien.	Ukraina, Ryssland.
Transportsektor	Ryssland, Tyskland.	Ukraina, Indien, Sverige, Nederländerna, USA.
Banksektor	Kina, Ryssland.	Ukraina, Ryssland.
Hälso- och sjukvårdssektor	Indien, Spanien, Storbritannien.	Ukraina, USA.
Tillagda sektorer		
Offentlig förvaltning	Kina, Indien, Ryssland, Sverige.	Ukraina.
Postsektor	Ryssland.	Ukraina.

3.1 Konsekvenser av WannaCry: incidenter och störningar

Detta kapitel redogör för vilka konsekvenser WannaCry lett till i länderna Indien, Kina, Ryssland, Spanien, Storbritannien, Sverige och Tyskland. I varje delkapitel redovisas ett land, med en inledande tabell som ger översikt över WannaCrys spridning och konsekvens i drabbade sektorer.

[62] COM 2017/476: MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET: Maximalt utnyttjande av it-säkerhetsdirektivet – mot ett effektivt genomförande av direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks och informationssystem i hela unionen. Bilaga, s. 23-24.

3.1.1 Indien

Tabell 2. WannaCrys spridning och konsekvenser i Indien.

Sektor	Spridning	Konsekvens
Energisektor	West Bengal State Electricity Distribution Company (WBSEDC) som levererar el till 96 procent av delstatens el-användare.[63]	Störningar i cirka en femtedel av WBSEDC:s betalningskontor. Långa köer och nedstängda kassor rapporterades.[64]
Hälso- och sjukvårds-sektor	Berhampur City Hospital i delstaten Odisha.	Störning i E-Audashi, ett affärssystem för inköp och lagerhållning av läkemedel och kirurgiska verktyg samt distribution av recept för mediciner. Störning i informationssystem som hanterar journaler, medicinska rapporter och andra dokument för sjukhuspersonal.[65]
Offentlig förvaltning	Andhra Pradesh polisväsende, 18 lokala polisorganisationer i 5 av 13 distrikt.[66]	System för hantering av brottsanmälningar blev otillgängligt. Vissa system stängdes av i preventivt syfte.[67]

Enligt mätningar av WannaCrys trafik var Indien det fjärde hårdast drabbade landet under utbrottet.[68] Samtidigt tros mörkertalet i rapporteringen vara stort, då det finns en kultur av att inte rapportera inträffade incidenter i landet.[69] Det kan dock konstateras att WannaCry spreds över flera sektorer, med negativ inverkan på tillgängligheten i nätverks- och informationssystemen som följd. Exempelvis drabbades faktureringssystemet i energisektorn i Västbengalen och sjukvårdssektorn i Odisha när det medicinska lagerhållningssystemet infekterades. Trots dessa incidenter är det inte tydligt att tillhandahållandet av den primära tjänsten i sig påverkades.

[63] *Hindustan Times*. "'WannaCry' ransomware: Bengal power distribution company hit by cyberattack, say officials, say officials", 2017-05-15.
https://www.hindustantimes.com/india-news/wannacry-ransomware-bengal-power-distribution-company-hit-by-cyberattack-say-officials/story-biqMQN5cPKng36cIyho2oJ.html [Hämtad: 2019-01-10].

[64] *NDTV*, "More Computers In Bengal's Electricity Distribution Offices Attacked By 'Wannacry", 2017-05-16. https://www.ndtv.com/india-news/more-computers-in-west-bengal-state-electricity-distribution-companys-offices-attacked-by-wannacry-1694383 [Hämtad: 2019-01-10]; *Hindustan Times*. "'WannaCry' ransomware: Bengal power distribution company hit by cyberattack, say officials, say officials", 2017-05-15.
https://www.hindustantimes.com/india-news/wannacry-ransomware-bengal-power-distribution-company-hit-by-cyberattack-say-officials/story-biqMQN5cPKng36cIyho2oJ.html [Hämtad: 2019-01-10].

[65] *LiveMint*, "Ransomware Attack: Odisha's govt hospital falls prey to WannaCry virus", 2017-05-17.
https://www.livemint.com/Technology/X76bZbPH4nN4w7MaXN6tZL/Ransomware-attack-Odishas-govt-hospital-falls-prey-to-Wann.html [Hämtad: 2019-01-10]; *DailyHunt*, "Ransomware attack: Govt hospitals continue to fall prey", 2017-05-20. https://m.dailyhunt.in/news/india/english/odishatv-epaper-odishatv/ransomware+attack+govt+hospitals+continue+to+fall+prey-newsid-67878733 [Hämtad: 2019-01-10].

[66] *Hindustan Times*. "WannaCry ransomware: Andhra police fall prey to global cyber attack", 2017-05-16. https://www.hindustantimes.com/india-news/wannacry-ransomware-andhra-police-fall-prey-to-global-cyber-attack/story-FkQZQHepiIAlVMJTobKLfN.html [Hämtad]

[67] IANS. "Andhra Pradesh's police departments affected by 'WannaCry' ransomware". *BGR*, 2017-05-16. https://www.bgr.in/news/andhra-pradeshs-police-departments-affected-by-wannacry-ransomware/ [Hämtad: 2019-03-29].

[68] Cimpanu, Catalin. "New Data Shows Most WannaCry Victims Are From China, Not Russia". *Bleeping Computer*. https://www.bleepingcomputer.com/news/security/new-data-shows-most-wannacry-victims-are-from-china-not-russia/ [Hämtad: 2019-02-05].

[69] ET Bureau. "India third worst hit nation by ransomware Wannacry; over 40,000 computers affected". *The Economic Times,* 2017-05-17. https://economictimes.indiatimes.com/tech/internet/india-third-worst-hit-nation-by-ransomware-wannacry-over-40000-computers-affected/articleshow/58707260.cms [Hämtad: 2019-02-05].

Landets före detta underrättelsechef betonade att bristfälliga rutiner för uppdatering av hård- och mjukvara, samt otillräcklig cyberhygien gjort landet mer utsatt.[70] Andra källor har också diskuterat det utbredda användandet av Windows XP som en viktig orsak. Microsoft underhöll vid tidpunkten för WannaCry inte längre Windows XP. Därför hade operativsystemet inte fått någon säkerhetsuppdatering mot de sårbarheter som WannaCry utnyttjade.[71] Just dessa två säkerhetsproblem framstod som särskilt viktiga för hur den indiska statsapparatens bemötte WannaCry. På nationell nivå meddelade den indiska regeringen den 13:e maj att man instruerat CERT-IN[72] att utreda situationen och samma dag utkom CERT-IN med rekommendationer på proaktiva och reaktiva åtgärder.[73] Bland annat rekommenderades att installera Windows senaste säkerhetsuppdatering och att skapa säkerhetskopior av kritisk data. Indikatorer för att se om ett system blivit infekterat samt instruktioner för hur man undgår gisslanprogram fanns också att tillgå.[74] Ministeriet för IT och elektronik kontaktade både offentliga och privata aktörer för att uppmana dessa att följa CERT-IN:s instruktioner. Ministeriet bad dessutom Microsoft Indien att gå ut med information om att installera säkerhetsuppdateringar.[75]

Även på lokal- och delstatsnivå reagerade myndigheterna skyndsamt. I Västbengalen, där elsektorn drabbades, gav myndigheterna ansvariga aktörer i uppdrag att ta fram nya säkerhetsföreskrifter och verksamheter uppmanades att säkerställa regelbundna uppdateringar av operativsystem och applikationer, så som de uppdateringar som rekommenderats i Microsofts senaste säkerhetsbulletin.[76]

I Odisha, där sjukvårdssektorn drabbats, utfärdade delstatens IT-minister den 16:e maj tjugo åtgärdsrekommendationer. Bland annat poängterades betydelsen av att kontinuerligt uppdatera anti-virusprogram, att avinstallera piratkopierade operativsystem till förmån för licensierade system, att tillämpa den senaste säkerhetsuppdateringen för Windows och att säkerhetskopiera viktig information i förebyggande syfte.[77] Utöver detta påbörjades arbetet med en förteckning över gamla och ny IT-system i delstaten. [78] Den lokala polisutredning som inletts lyftes upp till delstatsnivå och en specialgrupp bestående av experter på cyberbrottslighet tillsattes.[79] Sjukhusen besöktes av specialister från det nationella IT-centret

[70] *The Hindu*. 'WannaCry impact on India under-reported'. 2017-11-17. https://www.thehindu.com/news/cities/bangalore/wannacry-impact-on-india-under-reported/article20542868.ece [Hämtad: 2019-02-05].
[71] *Indian Express*. "WannaCry ransomware: Computers at West Bengal State electricity firm hit". 2017-05-15. https://indianexpress.com/article/technology/tech-news-technology/wannacry-ransomware-computers-at-west-bengal-state-electricity-firm-hit/ [Hämtad: 2019-02-05].
[72] Computer Emergency Response Team, har ofta till uppdrag att samordna och sprida information vid it-incidenter, se exempelvis: CERT-SE. "Om CERT-SE". 2019-01-22. https://www.cert.se/om-cert-se [Hämtad: 2019-03-27].
[73] Press Trust of India, "Government Activates Response Mechanism To Prevent Cyber Attack". *NDTV*, 2017-05-14. https://www.ndtv.com/india-news/government-activates-response-mechanism-to-prevent-cyber-attack-1693438 [Hämtad: 2019-02-05].
[74] CERT-IN. "Advisory CIAD-2017-0024. Wannacry/ WannaCrypt Ransomware – CRITICAL ALERT". 2017-05-14. Tillgänglig på https://www.cert-in.org.in/. [Hämtad: 2019-03-27].
[75] *Indian Express*. "WannaCry ransomware: Computers at West Bengal State electricity firm hit". 2017-05-15. https://indianexpress.com/article/technology/tech-news-technology/wannacry-ransomware-computers-at-west-bengal-state-electricity-firm-hit/ [Hämtad: 2019-02-05].
[76] *NDTV*, "More Computers In Bengal's Electricity Distribution Offices Attacked By 'Wannacry". 2017-05-16. https://www.ndtv.com/india-news/more-computers-in-west-bengal-state-electricity-distribution-companys-offices-attacked-by-wannacry-1694383 [Hämtad: 2019-01-10]
[77] Das, Lalit. "The advisory for Ransomware Threat-'WannaCry'". Government of Odisha Home Department. http://www.homeodisha.gov.in/sites/default/files/AddFiles/WANNACRY.pdf [Hämtad: 2019-03-27].
[78] *LiveMint*, "Ransomware Attack: Odisha's govt hospital falls prey to WannaCry virus". 2017-05-17. https://www.livemint.com/Technology/X76bZbPH4nN4w7MaXN6tZL/Ransomware-attack-Odishas-govt-hospital-falls-prey-to-Wann.html [Hämtad: 2019-01-10]
[79] Press Trust of India, "Ransomware Attack: Odisha's govt hospital falls prey to WannaCry virus". *LiveMint*, 2017-05-17. https://www.livemint.com/Technology/X76bZbPH4nN4w7MaXN6tZL/Ransomware-attack-Odishas-govt-hospital-falls-prey-to-Wann.html [Hämtad: 2019-01-10].

National Informatics Centre (NIC).[80] Slutligen satte delstaten upp ett speciellt telefonnummer för att sprida kunskap och råd rörande WannaCry.[81]

Polismyndigheten i Andhra Pradesh, som också drabbades av WannaCry, kunde senare bekräfta att konsekvenserna av infektionen varit minimala. Detta berodde främst på att alla polisen haft offline-kopior av både polisanmälningar och andra viktiga dokument.[82]

3.1.2 Kina

Tabell 3. WannaCrys spridning och konsekvenser i Kina.

Sektor	Spridning	Konsekvens
Banksektor	Bank of China.	Bankomater otillgängliga.[83]
Offentlig förvaltning	Bostadsfond i Zhuhai. Changsha stads socialtjänst. Tillsynsmyndighet för industrisektorn i Xuzhou. Dalians förvaltning för exit-entry som ger tillstånd för resor mellan fastlandet och Kinas speciella administrativa regioner.	Störningar i myndigheternas förmåga att och ta emot ansökningar.[84]

Vid WannaCrys utbrott fanns initialt farhågor om att kinesiska organisationer skulle drabbas kraftigt och att spridningen skulle vara aggressiv. Kryptomaskens spridningshastighet beskrevs ett par dagar efter utbrottet ha varit lägre än befarad.[85] Medierapporteringen tyder ändå på att spridningen i landet trots allt var utbredd. Enligt statistik från Kryptos Logic, var Kina det land där flest datorer infekterades av WannaCry.[86] Orsaker tros vara att det finns en betydande mängd datorer i Kina och att piratkopiering av Windows är vanligt: i en rapport från 2016 angavs att 70 procent av kinesiska datorer använder piratkopierade operativsystem.[87] Dessa versioner blir med tiden sårbara då de inte kan uppdateras när nya

DNA India, ”Odisha: City hospital system down, officials fear 'WannaCry' attack”. 2017-05-17. https://www.dnaindia.com/india/report-odisha-city-hospital-system-down-officials-fear-wannacry-attack-2441803 [Häntdatum: 2019-02-05].

[81] *Odisha Sun Times*, “Odisha govt issues advisory on WannaCry Ransomware”. 2017-05-17. https://odishasuntimes.com/odisha-govt-issues-advisory-on-wannacry-ransomware/ [Hämtad: 2019-02-05].

[82] *FactorDaily*, ”Worldwide ’WannaCry’ ransomware attack hit Andhra Police systems as well”. 2017-05-13. https://factordaily.com/news/wannacry-ransomware-andhra-police/ [Hämtad: 2019-01-10].

[83] Richter, Wolf. “China's use of pirated software left it vulnerable to the WannaCry ransomware attack”. *Business Insider*, 2017-05-16. https://www.businessinsider.com/wannacry-ransomware-attack-china-2017-5?r=US&IR=T&IR=T [Hämtad: 2019-02-05]

[84] Cadell, Cate; Jourdan, Adam och Gopalakrishnan, Raju. “Cyber attack hits China government, schools, but spread slows”. *Reuters*, 2017-05-15. https://www.reuters.com/article/us-cyber-attack-china-idUSKCN18B10H [Hämtad: 2019-02-05]

[85] Ibid.; Hersey, Frank. “Here’s what we know about how WannaCry has affected China”. *TechNode*, 2017-05-15. https://technode.com/2017/05/15/how-hard-did-wannacry-virus-hit-china/ [Hämtad: 2019-02-05]

[86] Cimpanu, Catalin. “New Data Shows Most WannaCry Victims Are From China, Not Russia”. *Bleeping Computer*. https://www.bleepingcomputer.com/news/security/new-data-shows-most-wannacry-victims-are-from-china-not-russia/ [Hämtad: 2019-02-05]

[87] Richter, Wolf. “China's use of pirated software left it vulnerable to the WannaCry ransomware attack”. *Business Insider*, 2017-05-16. https://www.businessinsider.com/wannacry-ransomware-attack-china-2017-5?r=US&IR=T&IR=T [Hämtad: 2019-02-05]

säkerhetsuppdateringar släpps.[88] Säkerhetsuppdateringar är också ofta lågt prioriterade då landet saknar tidigare erfarenhet av större incidenter.[89]

Den 17:e maj bekräftade Kinas tillsynsmyndighet för banksektorn, att sektorn var drabbad men att spridningen varit mindre än befarad. De angav även att inga incidentrapporter om större infektioner mottagits från någon av landets banker.[90] Däremot hade bankomater tillhörande Bank of China blivit infekterade och följaktligen otillgängliga.[91] Hur många användare som drabbades, vilken geografisk spridning eller vilken samhällelig och ekonomisk inverkan otillgängligheten fick är oklart. Med anledning av WannaCry-utbrottet beordrade ett antal nationella tillsynsmyndigheter att banker, fondbolag och lokala banktillsynsmyndigheter skulle genomföra självbesiktningar samt vidta åtgärder för att säkra sina IT-system.[92] Den nationella tillsynsmyndigheten för bankväsendet meddelade också att man arbetade med att ta fram en ny vägledning för cybersäkerhet i banksektorn.[93]

Även om utfallet alltså varit mindre än förväntat, rapporteras incidenter från flera offentliga förvaltningar, bland annat en bostadsfond i staden Zhuhai, staden Changshas socialtjänst, en tillsynsmyndighet för industrisektorn i Xuzhou samt staden Dalians förvaltning för exit-entry, som ger tillstånd för resor mellan fastlandet och Kinas speciella administrativa regioner.

[88] Lam, Oiwan. ”Why is China Home to Half of the Computers Infected With WannaCry Ransomware?”, *GlobalVoices Advox*, 2017-05-16. https://advox.globalvoices.org/2017/05/16/why-is-china-home-to-half-of-the-computers-infected-with-wannacry-ransomware/ [Hämtad: 2019-02-05]

[89] Cadell, Cate; Jourdan, Adam och Gopalakrishnan, Raju. “Cyber attack hits China government, schools, but spread slows”. *Reuters*, 2017-05-15. https://www.reuters.com/article/us-cyber-attack-china-idUSKCN18B10H [Hämtad: 2019-02-05]

[90] *Reuters*. ”China's banking regulator to step up protection after cyber attack”. 2017-05-17. https://www.reuters.com/article/us-cyber-attack-china-regulator/chinas-banking-regulator-to-step-up-protection-after-cyber-attack-idUSKCN18D0WZ [Hämtad: 2019-02-05]

[91] Richter, Wolf. “China's use of pirated software left it vulnerable to the WannaCry ransomware attack”. *Business Insider*, 2017-05-16. https://www.businessinsider.com/wannacry-ransomware-attack-china-2017-5?r=US&IR=T&IR=T [Hämtad: 2019-02-05]

[92] Hersey, Frank. “Here’s what we know about how WannaCry has affected China”. *TechNode*, 2017-05-15. https://technode.com/2017/05/15/how-hard-did-wannacry-virus-hit-china/ [Hämtad: 2019-02-05]

[93] *Reuters*. ”China's banking regulator to step up protection after cyber attack”. 2017-05-17. https://www.reuters.com/article/us-cyber-attack-china-regulator/chinas-banking-regulator-to-step-up-protection-after-cyber-attack-idUSKCN18D0WZ [Hämtad: 2019-02-05]

3.1.3 Ryssland

Tabell 4. WannaCrys spridning och konsekvenser i Ryssland.

Sektor	Spridning	Konsekvens
Transportsektor	Russian Railways.	Infektion men inga störningar rapporterade.[94]
Banksektor	Sberbank, Rysslands största bank.[95]	Infektion men inga störningar rapporterade.[96]
	Ryska centralbanken.	Infektion men inga störningar rapporterade.[97]
Offentlig förvaltning	Inrikesministeriet.	Ministeriet hävdade att 1 % av systemen blivit påverkade,[98] senare rapportering nämner ca 1000 datorer.[99] I flera regioner ska polisen haft problem att utfärda körkort eller registreringsnummer för fordon.[100]
Postsektor	Russian Post.	Talesperson förnekade att organisationen påverkades och menade att ett fåtal datorer stängts ner i förebyggande syfte.[101] Anställda menade dock att en mängd system infekterats, främst terminaler för kösystem på lokala postkontor som då fick stängas av.[102]

Sammanlagt beräknas 20 procent av alla infekterade WannaCry-datorer ha funnits i Ryssland.[103] Den internationella medierapporteringen om incidenterna i Ryssland ger främst en bild av spridning inom bank- och transportsektorerna samt inom offentlig administration och postverksamhet.

Användningen av föråldrade system gjorde Ryssland särskilt sårbart.[104] Utbredd piratkopiering av mjukvara är en annan faktor som gjorde det lättare för WannaCry att spridas i landet, då säkerhetsuppdateringar inte erbjuds för icke-licensierad mjukvara. Användningen

[94] *RT*. ”Russian banks, railway giant among targets of WannaCry ransomware allegedly linked to NSA”. 2017-05-13. https://www.rt.com/news/388228-wannacry-russian-railways-banks/ [Hämtad: 2019-03-29].
[95] Winning, Alexander och Stubbs, Jack. ”WannaCry cyber attack compromised some Russian banks: central bank”. *Reuters*, 2017-05-19. https://www.reuters.com/article/us-cyber-attack-russia-cenbank-idUSKCN18F16V [Hämtad: 2019-02-05].
[96] Ibid.
[97] Ibid.
[98] Wattles, Jackie och Disis, Jill. “Ransomware attack: Who's been hit been hit”. *CNN*, 2017-05-15. https://money.cnn.com/2017/05/15/technology/ransomware-whos-been-hit/index.html [Hämtad: 2019-02-05].
[99] Carrie Wong, Julia och Solon, Olivia. ”Massive ransomware cyber-attack hits nearly 100 countries around the world”. *The Guardian*, 2017-05-12. https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs [Hämtad: 2019-02-06].
[100] Yegorov, Oleg. “WannaCry hack: Why has Russia suffered more than other countries?”. *Russia Beyond*, 2017-05-16. https://www.rbth.com/international/2017/05/16/wannacry-hack-why-has-russia-suffered-more-than-other-countries_763869 [Hämtad: 2019-03-29]002E
[101] Stubbs, Jack. “Russian postal service brought down by WannaCry ransomware virus”. *The Independent*, 2017-05-25. https://www.independent.co.uk/life-style/gadgets-and-tech/news/russia-postal-service-wannacry-ransomware-cyber-virus-attack-windows-xp-a7754841.html [Hämtad: 2019-02-06].
[102] Moore-Colyer, Roland. “WannaCry Wallops Russian Post, Highlightning The Risk Of Legacy IT”. *Silicon*, 2017-05-25. https://www.silicon.co.uk/security/wannacry-russian-post-213099 [Hämtad: 2019-03-27].
[103] Stubbs, Jack. “Russian postal service brought down by WannaCry ransomware virus”. *The Independent*, 2017-05-25. https://www.independent.co.uk/life-style/gadgets-and-tech/news/russia-postal-service-wannacry-ransomware-cyber-virus-attack-windows-xp-a7754841.html [Hämtad: 2019-02-06].
[104] Kottasová, Ivana. ”Why Russia's cyber defenses are so weak”. *CNN*, 2015-05-15. https://money.cnn.com/2017/05/15/technology/russia-vulnerable-cyberattack/index.html [Hämtad: 2019-02-06].

av piratkopierad mjukvara i Ryssland uppskattades 2015 uppgå till 64 procent – att jämföra med det globala snittet på 39 procent.[105] Det framgår däremot inte om angreppet påverkade leveransen av någon primär leverans eller om det hade mer omfattande betydelse för samhällets säkerhet.

Den ryska centralbanken uppgav den 19:e maj att landets banksektor hade påverkats av WannaCry, även om konsekvenserna inte varit särskilt allvarliga. Rysslands största bank, Sberbank, uppgavs till exempel ha utsatts för WannaCry.[106] Banken hävdade dock att incidenten inte föranlett några störningar.[107] Antivirusföretaget Kaspersky Labs menade att inga kritiska banksystem i Ryssland hade drabbats och att det främst rörde sig om anställdas egna datorer.[108] Rysslands centralbank gav till följd av WannaCry ut rekommendationer till landets banker. Bland annat återupprepades en rekommendation från april 2017 om att säkerhetsuppdatera alla Windows-operativsystem. Centralbanken meddelade också att nyheter om cyberattacker och IT-säkerhet nu skulle börja publiceras på bankens hemsida.[109]

Det statliga järnvägsbolaget Russian Railways, vars system infekterades den 12:e maj, meddelade att det rörde sig om ett mindre antal krypterade datorer och att inga verksamhetskritiska filer skadats.[110] Inga störningar i tågtrafiken ska ha uppstått till följd av incidenten.[111] Vissa inom Russian Railways menar att störningarna minimerades av ren slump, då de flesta datorerna råkade vara avstänga just när incidenten började.[112] Russian Railways incidenthantering ska även ha påbörjats i ett tidigt skede, vilket gjorde att man både kunde isolera de infekterade systemen och uppgradera virusskydd för övriga datorer.[113]

Även ryska statsinstitutioner påverkades under de första timmarna av WannaCry:s utbrott den 12:e maj; exempelvis ska det ryska inrikesministeriet ha fått ett antal datorer infekterade.[114] Ministeriet hävdade att man endast behövt åtgärda ett mindre antal datorer[115] även om infektionen bedöms ha kunnat påverka upp till 1000 datorer.[116] Konsekvenserna ska ha varit marginella då de system som drabbades endast utgjorde en procent av ministeriets

[105] Stubbs, Jack. "Exclusive: Wannacry hits Russian postal service, exposes wider security shortcomings". *Reuters*, 2017-05-24. https://uk.reuters.com/article/us-cyber-attack-russia/exclusive-wannacry-hits-russian-postal-service-exposes-wider-security-shortcomings-idUKKBN18K26O [Hämtad: 2019-02-06].

[106] Winning, Alexander och Stubbs, Jack. "WannaCry cyber attack compromised some Russian banks: central bank". *Reuters*, 2017-05-19. https://www.reuters.com/article/us-cyber-attack-russia-cenbank-idUSKCN18F16V [Hämtad: 2019-02-05].

[107] Winning, Alexander och Stubbs, Jack. "WannaCry cyber attack compromised some Russian banks: central bank". *Reuters*, 2017-05-19. https://www.reuters.com/article/us-cyber-attack-russia-cenbank-idUSKCN18F16V [Hämtad: 2019-02-05].

[108] Ibid.

[109] Ibid.

[110] Wattles, Jackie och Disis, Jill. "Ransomware attack: Who's been hit been hit". *CNN*, 2017-05-15. https://money.cnn.com/2017/05/15/technology/ransomware-whos-been-hit/index.html [Hämtad: 2019-02-05].

[111] *RT*. " Russian banks, railway giant among targets of WannaCry ransomware allegedly linked to NSA". 2017-05-13. https://www.rt.com/news/388228-wannacry-russian-railways-banks/ [Hämtad: 2019-02-05].

[112] Stubbs, Jack. "Russia still reeling from WannaCry ransomware attack". *Business Live*, 2017-05-25. https://www.businesslive.co.za/bd/world/europe/2017-05-25-russia-still-reeling-from-wannacry-ransomware-attack/ [Hämtad: 2019-02-05].

[113] Wattles, Jackie och Disis, Jill. "Ransomware attack: Who's been hit". *CNN*, 2017-05-15. https://money.cnn.com/2017/05/15/technology/ransomware-whos-been-hit/index.html [Hämtad: 2019-02-05].

[114] Ibid.

[115] Ibid.

[116] Carrie Wong, Julia och Solon, Olivia. "Massive ransomware cyber-attack hits nearly 100 countries around the world". *The Guardian*, 2017-05-12. https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs [Hämtad: 2019-02-06].

datornätverk.[117] Framför allt drabbades inga av ministeriets servrar, då dessa använder inhemska operativsystem.[118] Rysslands president Vladimir Putin betonade också att ingen av landets institutioner åsamkats någon betydande skada.[119]

Det är oklart till vilken utsträckning statliga postoperatören Russian Post drabbades av WannaCry.[120] En talesperson från Russian Post menade att inga system infekterats, men att vissa system stängts av i förebyggande syfte. Anställda inom Russian Post menade istället att en mängd datorer infekteras, främst datorer som används som terminaler för kösystem på lokala postkontor.[121] Anledningen till infektionen angavs vara att terminalerna använt Windows XP.[122]

3.1.4 Spanien

Tabell 5. WannaCrys spridning och konsekvenser i Spanien.

Sektor	Spridning	Konsekvens
Hälso- och sjukvårds-sektor	Två sjukhus i Bilbao och Salamanca.	Störningar i tjänster på interna nätverk men ingen påverkan på patientvården.[123]
Energisektor	Gas Natural.[124]	Begränsad infektion. System stängdes ner i förebyggande syfte.
	Iberdrola[125], landets största elproducent.[126]	System stängdes ner i förebyggande syfte.

Redan den 12:e maj indikerade tidig statistik om WannaCry från Kaspersky Labs att Spanien var ett av de 20 länder där flest datorer infekterats.[127] Tre dagar senare bekräftade det nationella cyberinstitutet INCIBE i ett uttalande att de identifierat 1200 kända infektioner i

[117] Yegorov, Olev. "WannaCry hack: Why has Russia suffered more than other countries?". *Russia Beyond*, 2017-05-16. https://www.rbth.com/international/2017/05/16/wannacry-hack-why-has-russia-suffered-more-than-other-countries_763869 [Hämtad: 2019-02-06].

[118] *BBC*. "Ransomware cyber-attack: Who has been hardest hit?". 2017-05-15. https://www.bbc.com/news/world-39919249 [Hämtad: 2019-02-06].

[119] Kottasová, Ivana. "Why Russia's cyber defenses are so weak". *CNN*, 2015-05-15. https://money.cnn.com/2017/05/15/technology/russia-vulnerable-cyberattack/index.html [Hämtad: 2019-02-06].

[120] Stubbs, Jack. "Exclusive: Wannacry hits Russian postal service, exposes wider security shortcomings". *Reuters*, 2017-05-24. https://uk.reuters.com/article/us-cyber-attack-russia/exclusive-wannacry-hits-russian-postal-service-exposes-wider-security-shortcomings-idUKKBN18K26O [Hämtad: 2019-02-06]; Stubbs, Jack. "Russian postal service brought down by WannaCry ransomware virus". *The Independent*, 2017-05-25. https://www.independent.co.uk/life-style/gadgets-and-tech/news/russia-postal-service-wannacry-ransomware-cyber-virus-attack-windows-xp-a7754841.html [Hämtad: 2019-02-06].

[121] Stubbs, Jack. "Exclusive: Wannacry hits Russian postal service, exposes wider security shortcomings". *Reuters*, 2017-05-24. https://uk.reuters.com/article/us-cyber-attack-russia/exclusive-wannacry-hits-russian-postal-service-exposes-wider-security-shortcomings-idUKKBN18K26O [Hämtad: 2019-02-06]; Stubbs, Jack. "Russian postal service brought down by WannaCry ransomware virus". *The Independent*, 2017-05-25. https://www.independent.co.uk/life-style/gadgets-and-tech/news/russia-postal-service-wannacry-ransomware-cyber-virus-attack-windows-xp-a7754841.html

[122] Moore-Colyer, Roland. "WannaCry Wallops Russian Post, Highlightning The Risk Of Legacy IT". *Silicon*, 2017-05-25. https://www.silicon.co.uk/security/wannacry-russian-post-213099 [Hämtad: 2019-03-27].

[123] Urra, Susanna. "How the WannaCry ransomware attack affected businesses in Spain". *El País*, 2017-05-19. https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [Hämtad: 2019-02-06].

[124] Goodin, Dan. "An NSA-derived ransomware worm is shutting down computers worldwide". *ArsTechnica*, 2017-05-12. https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/ [Hämtad: 2019-04-01].

[125] Ibid.

[126] Smart Energy International. "Iberdrola Producing more MWs in Mexico than Spain for 2018". 2018-07-31. https://www.power-eng.com/articles/2018/07/iberdrola-producing-more-mws-in-mexico-than-spain-for-2018.html [Hämtad: 2019-04-01].

[127] Bazaraa, Danya. "These are the '74 countries hit by 45,000 WannaCry cyber attacks - and Russia is worst affected"'. *The Mirror*, 2017-05-15. https://www.mirror.co.uk/tech/74-countries-hit-45000-wannacry-10411971 [Hämtad: 2019-02-06].

Spanien.[128] Spanien var alltså ett av de första (kända) länderna att drabbas av WannaCry-utbrottet.[129]

Ett antal organisationer inom sjukvårdssektorn och energisektorn tros ha drabbats, även om information om konsekvenserna är relativt knapphändig.[130] Vissa lokala utredare har pekat på bristande transparens om incidenterna i Spanien och bedömer att många som påverkats inte har rapporterat incidenterna.[131]

Redan under WannaCrys första spridningsdag varnade den spanska CERT:en för WannaCry och rekommenderade åtgärder för att förhindra utbrott och hantera infekterade system.[132] Användare rekommenderades att stänga av de nätverksportar som WannaCry nyttjade samt att installera säkerhetsuppdateringar. Datorer som inte kunde uppdateras skulle stängas av eller isoleras. Offren avråddes även från att betala lösensumman och uppmanades att spara krypterade filer efter att systemens funktionalitet återupprättats, i händelse av att krypteringsnycklar för WannaCry senare skulle offentliggöras.[133]

Sjukhusanställda vid sjukhus i Bilbao och i Salamanca uppgav till dagstidningen El Pais att flera tjänster på deras interna nätverk påverkats av WannaCry men att det inte hade haft några konsekvenser för patientvården. Övriga vårdinrättningar som tidningen kontaktade rapporterade att de använde Windows 7, ett operativsystem där säkerhetsuppdateringarna förebyggt infektion.[134]

I media rapporterades också att WannaCry drabbat två bolag inom den spanska energisektorn, landets största elproducent Iberdrola[135] och naturgasleverantören Gas Natural.[136] Det finns inga bekräftade störningar i företagens tjänsteleveranser.[137] På Gas Naturals Madrid-kontor ska personaldatorer ha visat tecken på infektion, vilket föranledde att samtliga anställda ombads att stänga av sina datorer. Även hos Iberdrola ska en mängd datorer ha stängts ner i förebyggande syfte.[138]

[128] Palazuelos, Félix. ” How the WannaCry ransomware attack affected businesses in Spain”. *El País*, 2017-05-19. https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [Hämtad: 2019-02-06].
[129] Urra, Susanna. ”How the WannaCry ransomware attack affected businesses in Spain”. *El País*, 2017-05-19. https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [Hämtad: 2019-02-06].
[130] Ruano, Carlos; Rodriguez, Jose; Finkle, Jim; White, Sarah; Berwick, Angus och Lawrence, Jane. “Telefonica, other Spanish firms hit in "ransomware" attack”. *Reuters*, 2017-05-12. https://www.reuters.com/article/us-spain-cyber/telefonica-other-spanish-firms-hit-in-ransomware-attack-idUSKBN1881TJ [Hämtad: 2019-02-06].
[131] Palazuelos, Félix. ” How the WannaCry ransomware attack affected businesses in Spain”. *El País*, 2017-05-19. https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [Hämtad: 2019-02-06].
[132] Goodin, Dan. “An NSA-derived ransomware worm is shutting down computers worldwide”. *Ars Technica*, 2017-05-12. https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/ [Hämtad: 2019-02-06].
[133] CCN-CERT. “Identificado ataque de ransomware que afecta a sistemas Windows“. 2017-05-12. https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html [Hämtad: 2019-02-06].
[134] Urra, Susanna. ”How the WannaCry ransomware attack affected businesses in Spain”. *El País*, 2017-05-19. https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [Hämtad: 2019-02-06].
[135] Smart Energy International. “Iberdrola Producing more MWs in Mexico than Spain for 2018”. 2018-07-31. https://www.power-eng.com/articles/2018/07/iberdrola-producing-more-mws-in-mexico-than-spain-for-2018.html [Hämtad: 2019-04-01].
[136]Alonso, Alejandro. “The Spanish Wholesale Gas Market”. National Energy Commission [Spanien], [Presentation], u.d. https://www.efet.org/Files/Documents/Press/Energy%20Trading%20Analyses/Third%20Party%20Publications//Presentacion%20CNE.pdf [Hämtad: 2019-02-06].
[137] Goodin, Dan. “An NSA-derived ransomware worm is shutting down computers worldwide”. *Ars Technica*, 2017-05-12. https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/ [Hämtad: 2019-02-06].
[138] Toledano, Bruno. ” Hackean la red interna de Telefónica y de otras grandes empresas españolas”. *El Mundo*, 2017-05-12. https://www.elmundo.es/tecnologia/2017/05/12/59158a8ce5fdea194f8b4616.html [Hämtad: 2019-02-06].

3.1.5 Storbritannien

Tabell 6. WannaCrys spridning och konsekvenser i Storbritannien.

Sektor	Spridning	Konsekvens
Hälso- och sjukvårds-sektorn	National Health Service.	Akutmottagningar fick omdirigera akutpatienter till närliggande sjukhus.[139] Patientbesök och återbesök ställdes in.[140] Mejlsystem och medicinteknisk utrustning stängdes av i förebyggande syfte.[141] Störningar i verksamheten då kliniska system och journalsystem inte var tillgängliga.[142]

Fredagen den 12:e maj, strax efter lunch, kom den första varningen från National Health Service (NHS, sjukvårdsansvarig myndighet i Storbritannien) egen CERT om att ett antal NHS-vårdenheter inom landets sjukvårdssektor drabbats av ett gisslanprogram. Varningen skickades från CareCERT, en CERT-funktion vid NHS Digital, som ansvarar för NHS IT-system. Senare under eftermiddagen hade utbrottet mer än fördubblats. NHS England förklarade vid klockan 16 händelsen som en stor nationell cyberincident. Först en vecka senare förklarades incidenten vara över.[143]

Det är främst inom engelsk sjukvård där konsekvenser för tjänsteleverans var tydliga. Av alla engelska sjukhus upplevde sammanlagt en tredjedel någon form av störningar under utbrottet. Sammanlagt ska en procent av NHS Englands verksamhet ha påverkats direkt av WannaCry.[144]

Störningarna innebar att patienter fick omdirigeras till närliggande sjukhus när akutmottagning inte kunde ta emot fler patienter. Det medförde att patienter fick färdas längre än normalt för akutvård. Omdirigeringarna varade fram tills den 16:e maj.[145] Totalt fick fem akutmottagningar omdirigera akutpatienter till närliggande sjukhus. Det finns dock ingen total uppskattning av hur många patienter som drabbades.[146]

Utöver störningar vid akutvården fick ett antal patient- och återbesök ställas in under den vecka som WannaCry-incidenten pågick.[147] NHS räknar med att 1,2 procent av alla inplanerade nya patientbesök (utanför akutvård) ställdes in.[148] Statistik över hur många återbesök som ställdes in saknas.[149]

[139] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 12 & 14. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[140] Ibid., s. 13.
[141] *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017., s. 13. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].
[142] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 14. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[143] Hughes, Owen. "WannaCry one year on: a retrospective look at NHS IT's black-letter day". *DigitalHealth.net*, 2018-05-11. https://www.digitalhealth.net/2018/05/wannacry-one-year-on/ [Hämtad: 2019-02-14].
[144]Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018 s. 5 & s. 14. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[145] Ibid., s. 12 & 14.
[146] Ibid.
[147] Ibid., s. 13.
[148] Ibid.
[149] National Audit Office. "*Investigation: WannaCry cyber attack and the NHS*". 2017, s. 8. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].

Utöver ökad arbetsbelastning för sjukvårdpersonal[150] orsakade WannaCry stora kostnader i form av övertid, kostnader för systemåterställning och ökad IT-support.[151] Även vårdenheter vars utrustning inte smittats, påverkades av incidenten. Många stängde exempelvis av mejlsystem och medicinteknisk apparatur i förebyggande syfte, vilket medförde både kommunikationssvårigheter och svårigheter att bedriva ordinarie verksamhet.[152] Verksamheten i många vårdenheter försvårades av att vissa kliniska system och journalsystem under perioder inte gick att nå.[153] Inga uppskattningar om omfattningen av dessa störningar har gjorts.[154] Däremot ska en procent av all NHS diagnostiska utrustning ha infekterats av WannaCry.[155] Inga patientdata anses ha blivit stulen eller äventyrad.[156]

NHS hanterande incidenten via sin EPRR-modell (*Emergency, Preparedness, Resilience* and *Response*). Hanteringen följde tre faser:

- under fas ett, som varade från den 12:e maj till 14:e maj, fokuserade NHS främst på att säkerställa akutsjukvården
- under fast två, mellan den 13:e och 15:e maj, säkerställdes att primärvården fungerade stabilt
- under den tredje och avslutande fasen fram till avslutandet av incidenten den 19:e maj, gjordes löpande reparationer av system och virusskydd uppdaterades.[157]

Den 17:e maj hade 95 procent av alla vårdenheter som drabbats av infektioner återgått till full funktionalitet och den 19:e maj hade samtliga påverkade vårdinrättningar återhämtat sig.[158]

Efterföljande utredningar identifierande ett antal omständigheter som försvårade återhämtningen. Det var inledningsvis svårt att upprätta en lägesbild i och med att WannaCry skapade störningar i många delar av NHS. Svårigheter i att inledningsvis koordinera hanteringen kopplas också till otydligheter kring var enheter skulle rapportera in incidenter: till NHS nationellt, socialdepartementet eller direkt till polisen.[159] Lokala vårdenheter fick lägga mycket tid på att besvara flera likartade förfrågningar från olika instanser. Dessutom försvårades kommunikationen av att många vårdenheter drog in möjligheten att skicka

[150] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, 2018, s. 34. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[151] National Audit Office, 2017. "*Investigation: WannaCry cyber attack and the NHS*", s. 8 & 15. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].
[152] Ibid., s. 13.
[153] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 14. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[154] National Audit Office, 2017. "*Investigation: WannaCry cyber attack and the NHS*", s. 7. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].
[155]Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 5 & s. 14. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[156] Ibid., s. 5.
[157] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 10. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[158] Ibid.
[159]*Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017., s. 24. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].

mejl utanför sin egen lokala vårdenhet.[160] Därför fick personal gå över till att kommunicera med personliga telefoner via bland annat meddelandeapplikationen WhatsApp.[161] Lärdomarna har bland annat lett till nya rutiner för kommunikation och utbyte av information mellan olika nivåer inom NHS i händelse av kris.[162] Hanteringen av WannaCry påvisade också att den planering som fanns på departementsnivå för cyberangrepp inte var lokalt inövad eller förankrad.[163]

En annan identifierad brist var att lokala vårdenheter inte följt tidigare rekommendationer om åtgärder mot sårbarheter. Bland annat fanns många vårdenheter som inte hade uppdaterat sina brandväggar eller genomfört nätverkssegmentering.[164] Det fanns inte heller mandat för NHS CERT eller NHS Digital (den funktion som bland annat ansvarar för IT-system hos vårdenheterna) att kräva att lokala vårdenheter vidtog säkerhetsåtgärder. Detta trots att NHS Digitals utvärderingar av lokal cybersäkerhet fram tills WannaCry gett samtliga 88 testade vårdenheter underkänt.[165] De vårdenheter som hörsammade säkerhetsrekommendationer var också ofta de som redan var mer ”cybermogna”, medan vårdenheter med låg cyberkompetens ofta fortsatte utsätta sig för sårbarheter.[166]

Ett annat problem var att flera typer av medicinteknisk utrustning som drabbades hanterades av underleverantörer. Som en konsekvens hade NHS begränsad insyn i vilka operativsystem som användes eller hur sårbara dessa var.[167] Systemen kommer ofta med ett inbyggt operativsystem och kan inte uppdateras av NHS-personal, utan måste underhållas av underleverantören.[168] Flera vårdenheter menar även att underleverantörernas hantering av WannaCry var långsam eller bristfällig.[169]

Sammantaget understryker de brittiska utredningarna att WannaCry hade kunnat hanteras bättre om NHS skött underhåll och hantering av sina IT-system bättre.[170] National Audit Office sammanfattar det som ett misslyckande med att uppdatera system, samt att man förlitade sig på gammal mjukvara.[171] NHS beskriver perioden innan WannaCry som präglad

[160] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 32-33. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[161] *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017., s. 6. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].
[162] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 31 & 33. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[163] *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017, s. 9. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].
[164] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 6 & 8. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[165] *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017, s. 6, 19-20. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].
[166] Ibid., s, 19.
[167] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 26. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[168] *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017. s. 18. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].
[169] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 26. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].
[170] Ibid., s. 23.
[171] *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017., s. 16. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].

av ”historiska underinvesteringar” i nätverkssäkerhet och ny mjukvara.[172] Utredningarna betonar bland annat att det på ledningsnivå måste tas större ansvar för området cybersäkerhet och att verksamheter måste få ökad förståelse för vilka risker cyberhot kan innebära för deras tjänsteleveranser. NHS uppmuntrades att vidta proaktiva åtgärder för att maximera sin resiliens och därmed minska potentiella negativa effekter för patientvården.[173] Ett förändrat tankesätt, som premierar systematisk utvärdering och hantering av potentiella hot från cyberattacker, rekommenderades även.[174]

3.1.6 Sverige

Tabell 7. WannaCrys spridning och konsekvenser i Sverige.

Sektor	Spridning	Konsekvens
Offentlig förvaltning	Timrå kommun.	Ett hundratal datorer blev otillgängliga, vilket påverkade administrativt arbete men inte leveransen av tjänster så som äldreomsorg eller hemtjänst.

Den 15:e maj, tre dagar efter WannaCry-utbrottet, konstaterades att Sverige varit relativt förskonat från utbrottets spridning.[175] Myndigheten för samhällsskydd och beredskap (MSB) uppgav att man inte fått några indikationer på att samhällsviktig verksamhet skulle ha drabbats.[176] Polisens Nationella operativa avdelning (NOA) gjorde även några dagar senare bedömningen att genomslaget i Sverige var betydligt lägre än i andra länder. Totalt hade NOA fått in färre än 10 polisanmälningar kopplade till WannaCry.[177] Sverige fanns inte heller med i Kaspersky Labs statistik över de tjugo länder som drabbats hårdast.[178] Flertalet informationschefer menar att deras verksamheter regelbundet installerar nya säkerhetsuppdateringar, vilket kan ha haft en förebyggande och minimerande effekt.[179] Bland de drabbade sektorerna i Sverige var det den offentliga sektorn (Timrå kommun) som påverkades av incidenten, med följdverkningar inom kommunal hälso- och sjukvård.

Redan fredagen den 12:e maj fick Timrå kommun ett hundratal datorer låsta till följd av WannaCry-utbrottet.[180] Kommunen menade att dess IT-leverantör försenat nödvändiga säkerhetsuppdateringar. Därför var kommunens system inte säkerhetsuppdaterade mot den sårbarhet som WannaCry utnyttjade. Även om det är oklart vilken ekonomisk inverkan

[172] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 8. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].

[173] *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017., s. 9-10. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].

[174] Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London: National Health Service, 2018, s. 6. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].

[175] TT. ”Ingen akut ökning av virusdrabbade”. *Ny Teknik*, 2017-05-15. https://www.nyteknik.se/digitalisering/ingen-akut-okning-av-virusdrabbade-6848426 [Hämtad: 2019-02-14].

[176] Myndigheten för samhällsskydd och beredskap. ”FAQ om WannaCry”. 2017-05-15. https://www.msb.se/sv/Insats--beredskap/Pagaende-handelser-och-insatser/Tidigare-handelser/IT-attacken-WannaCryransomware/FAQ-om-WannaCry/ [Hämtad: 2019-02-06].

[177] Wiklund, Kalle. ”Polisen: Så många svenskar har anmält Wannacry-utpressarna”. *Ny Teknik*, 2017-05-17. https://www.nyteknik.se/digitalisering/polisen-sa-manga-svenskar-har-anmalt-wannacry-utpressarna-6849119 [Hämtad: 2019-02-14].

[178] Bazaraa, Danya. “These are the '74 countries hit by 45,000 WannaCry cyber attacks - and Russia is worst affected'”. *The Mirror*, 2017-05-15. https://www.mirror.co.uk/tech/74-countries-hit-45000-wannacry-10411971 [Hämtad: 2019-02-14].

[179] Rosengren, Lina. ”Svenska cio:er: så klarade vi oss från Wannacry”. *IDG.se*, 2017-06-05. https://cio.idg.se/2.1782/1.683866/svenska-cioer-wannacry [Hämtad: 2019-02-14].

[180] Wiklund, Kalle. ”Timrå kommun: Miss hos it-leverantör öppnade för Wannacry”. *Ny Teknik*, 2017-05-17. https://www.nyteknik.se/digitalisering/timra-kommun-miss-hos-it-leverantor-oppnade-for-wannacry-6849137 [Hämtad: 2019-02-06].

WannaCry hade på Timrås kommun, krävde man IT-leverantören på närmare en miljon kronor i skadestånd.[181]

Kommunen underströk att utförandet av samhällelig verksamhet som äldreomsorg eller hemtjänst inte påverkats av WannaCry.[182] Kommunens hemtjänst, som utför cirka 1000 hembesök om dagen, ombads i förebyggande syfte att stänga av sina datorer och utföra arbetet manuellt med papper och penna.[183] Kommunen pekade på att rutiner redan fanns för att arbeta utan datorstöd inom vård och omsorg.[184] Personal inom hemtjänsten menar själva att alla hemtjänstbesök inplanerade den helgen kunde genomföras, men betonar samtidigt att situationen belyser strukturella sårbarheter och att man denna gång räddats av att papperskopior över helgens besöks- och arbetsscheman redan var utskrivna innan datorerna behövde stängas av.[185] Det som beskrivits som den främsta effekten på kommunens verksamhet var istället att administrativ personal inte kunde arbeta efter att deras datorer blivit låsta.[186]

3.1.7 Tyskland

Tabell 8. WannaCrys spridning och konsekvenser i Tyskland.

Sektor	Spridning	Konsekvens
Transportsektor	Deutsche Bahn.[187]	Informationstavlor och vissa biljettautomater ej tillgängliga.

Tysklands federala myndighet för informationssäkerhet (Bundesamt für Sicherheit in der Informationstechnik, BSI) ansåg att landet klarat sig väl från WannaCry.[188] Enligt myndighetens uppskattning var Tyskland det 13:e hårdast drabbade landet, vilket ansågs vara en relativ framgång och som en indikation på att tyska cybersäkerhetsåtgärder under senare år gett resultat. De tyska motåtgärderna mot WannaCry preciseras däremot inte närmare i rapporteringen.[189]

I Tyskland påverkades främst transportsektorn då system hos Deutsche Bahn (DB) infekterades med WannaCry.[190] DB är Tysklands i särklass största tågoperatör; 2017 uppgick DB:s marknadsandelar för regional tågtrafik och godstrafik inom landet till 67 respektive

[181] Lindblom, Hans. ”Timrå kommun hade gammalt virusskydd”. *SVT*, 2017-10-29. https://www.svt.se/nyheter/lokalt/vasternorrland/timra-kommun-hade-gammalt-virusskydd [Hämtad: 2019-02-14].
[182] Wiklund, Kalle. ”Timrå kommun: Miss hos it-leverantör öppnade för Wannacry”. *Ny Teknik*, 2017-05-17. https://www.nyteknik.se/digitalisering/timra-kommun-miss-hos-it-leverantor-oppnade-for-wannacry-6849137 [Hämtad: 2019-02-06].
[183] Israelsson, Fredrik. ”Personal på hemtjänsten fick ta fram papper och penna”. *SVT*, 2017-05-15. https://www.svt.se/nyheter/lokalt/vasternorrland/personalen-fick-ta-fram-papper-och-penna [Hämtad: 2019-02-14].
[184] Nekham, Erika. ”Ingen "måndagsvåg" av virusattacken”. *Norbottens Kuriren*, 2017-05-15. https://www.kuriren.nu/nyheter/ingen-mandagsvag-av-virusattacken-nm4545730.aspx [Hämtad: 2019-02-14].
[185] Israelsson, Fredrik. ”Personal på hemtjänsten fick ta fram papper och penna”. *SVT*, 2017-05-15. https://www.svt.se/nyheter/lokalt/vasternorrland/personalen-fick-ta-fram-papper-och-penna [Hämtad: 2019-02-14].
[186] Svensson, Anton och Quayle, Anna. ”Kommuner hårt drabbade av utpressningsvirus”. *SVT*, 2017-10-31. https://www.svt.se/nyheter/lokalt/vasternorrland/kommuner-hart-drabbade-av-utpressningsvirus [Hämtad: 2019-02-06].
[187] Nasr, Joseph och Heinrich, Mark. ”German rail operator affected by global cyber attack”. *Reuters*, 2017-05-13. https://www.reuters.com/article/us-cyber-attack-germany-rail-idUSKBN1890DM [Hämtad: 2019-02-14].
[188] *The State of IT Security in Germany 2017*. Bonn: Federal Office for Information Security (BSI), 2017. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2017.pdf?__blob=publicationFile&v=3 [Hämtad: 2019-02-14].
[189] Shalal, Andrea. “Germany's BSI says more German companies affected by cyber attacks”. *Reuters*, 2017-05-15. https://www.reuters.com/article/us-cyber-attack-germany/germanys-bsi-says-more-german-companies-affected-by-cyber-attacks-idUSKCN18B242 [Hämtad: 2019-02-14].
[190] Nasr, Joseph och Heinrich, Mark. ”German rail operator affected by global cyber attack”. *Reuters*, 2017-05-13. https://www.reuters.com/article/us-cyber-attack-germany-rail-idUSKBN1890DM [Hämtad: 2019-02-14].

68 procent.[191] De datorer som blev infekterade ska ha använt Windows XP och hade inte uppdaterats på flera år.[192] DB:s internutredning visar att organisationens CERT redan i ett tidigt skede sett tecken på infektion och försökt vidta åtgärder för att avskärma infekterade system. Eftersom DB saknade en tydlig incidenthanteringsplan misslyckades avskärmningsförsöket. Det gick inte heller att påbörja en full incidenthanteringsprocess då ansvarig personal inom organisationen inte kunde nås nattetid.[193]

Effekten av WannaCry var att DB:s informationsskärmar på flera håll i landet visade ett utpressningsmeddelande istället för avgångar och ankomster. Ett antal biljettautomater låstes också och blev oanvändbara.[194] Som en konsekvens fick resenärer svårare att tillgodogöra sig information om resor och anslutningar.[195] WannaCry ska inte ha orsakat några störningar för tågtrafik.[196]

3.2 Konsekvenser av NotPetya: incidenter och störningar

Följande kapitel redovisar inträffade händelser under spridningen av NotPetya. Först ger kapitlet en översikt över internationella incidenter för att sedan fokusera på Ukraina och Sverige.

Utanför Ukraina drabbades indiska[197], nederländska[198], svenska[199] och amerikanska[200] transportsektorerna, ryska energisektorn,[201] ryska banksektorn,[202] samt amerikanska hälso- och sjukvårdssektorn.[203] Således förefaller den internationella spridningen vara begränsad,

[191] Barrow, Keith. "German Monopoly Commission challenges DB dominance". *International Railway Journal*, 2017-09-01. https://www.railjournal.com/in_depth/german-monopoly-commission-challenges-db-dominance [Hämtad: 2019-02-14].
[192] Van Gompel, Marieke. "WannaCry virus was 'wake-up call' for railway industry". *RailTech.com*, 2017-12-11. https://www.railtech.com/all/2017/12/11/wannacry-virus-was-wake-up-call-for-railway-industry/ [Hämtad: 2019-02-14].
[193] Van Gompel, Marieke. "WannaCry virus was 'wake-up call' for railway industry". *RailTech.com*, 2017-12-11. https://www.railtech.com/all/2017/12/11/wannacry-virus-was-wake-up-call-for-railway-industry/ [Hämtad: 2019-02-14].
[194] AFP / The Local. "International cyber attacks put ransoms on German rail station screens". *The Local*, 2017-05-13. https://www.thelocal.de/20170513/international-cyber-attacks-put-ransoms-on-german-train-departure-boards [Hämtad: 2019-03-27]
[195] Samson, Adam; McGee, Patrick; Hornby, Lucy; Zhang, Archie; Fildes, Nic och Inagaki, Kana. "WannaCry cyber attack highlights dilemma in fight against malware". *Financial Times*, 2017-05-15. https://www.ft.com/content/bf29e8e0-3985-11e7-821a-6027b8a20f23 [Hämtad: 2019-02-14].
[196] Nasr, Joseph och Heinrich, Mark. "German rail operator affected by global cyber attack". *Reuters*, 2017-05-13. https://www.reuters.com/article/us-cyber-attack-germany-rail-idUSKBN1890DM [Hämtad: 2019-02-14].
[197] IANS. "Indian government has started taking measures to protect itself from the latest ransomware attack". *First Post*, 2017-06-28. https://www.firstpost.com/tech/news-analysis/indian-government-has-started-taking-measures-to-protect-itself-from-the-latest-ransomware-attack-3835135.html [Hämtad: 2019-02-18].
[198] Thomson, Iain. "Virus (cough, cough, Petya) goes postal at FedEx, shares halted". *The Register*, 2018-06-28. https://www.theregister.co.uk/2017/06/28/fedex_tnt_express_virus_attack/ [Hämtad: 2019-02-18]; *Port of Rotterdam*. "More vessels call on a safe port". 2018-01-15. https://www.portofrotterdam.com/en/news-and-press-releases/more-vessels-call-on-a-safe-port [Hämtad: 2019-02-18].
[199] Tenitskaja, Alexandra Carlsson och Dickson, Staffan. "Storföretag drabbade av nätattack". *Aftonbladet*, 2017-06-27. https://www.aftonbladet.se/nyheter/a/Ja618/hackerattack-mot-goteborgs-hamn [Hämtad: 2019-02-18].
[200] Burnson, Patrick. "Port of Los Angeles reacts to Petya Crisis as CargoSmart Provides Some Supply Chain Solutions". *Supply Chain Management Review*, 2017-06-28. http://www.scmr.com/article/port_of_los_angeles_reacts_to_pety_crisis_as_cargosmart_provides_some_suppl [Hämtad: 2019-03-27].
[201] *Offshore Energy Today*. "Maersk, Rosneft hit by cyberattack". 2017-06-28. https://www.offshoreenergy-today.com/report-maersk-rosneft-hit-by-cyberattack/ [Hämtad: 2019-02-18].
[202] Sulleyman, Aatif. "'Petya' cyber attack: list of affected companies shows scale of hack". *The Independent*, 2017-06-27. https://www.independent.co.uk/life-style/gadgets-and-tech/news/petya-cyber-attack-affected-companies-hack-wpp-rosneft-mondelez-deutsche-post-security-problems-a7811056.html [Hämtad: 2019-02-18].
[203] Glaser, April. "U.S hospitals have been hit by the global ransomware attack". *Recode*, 2017-06-27. https://www.recode.net/2017/6/27/15881666/global-eu-cyber-attack-us-hackers-nsa-hospitals [Hämtad: 2019-03-27].

men särskilt utbredd inom internationell transport. Detta beror på att det globala logistikkonglomeratet A.P. Møller-Maersk med dotterbolag drabbades särskilt hårt i ett flertal länder. Globalt beräknas störningarna av NotPetya orsakat upp till 10 miljarder US dollar i kostnader.[204]

När NotPetya väl brutit ut på ett lokalt kontor i Ukraina spred det sig i flera fall vidare till andra länder genom företagens långdistansnätverk som kopplar ihop företagens lokala nätverk över större geografiska områden.[205] Arne Schoenbohm, högste chef för tyska BSI menade i en intervju att i alla kända internationella fall hade infektionen kommit från ukrainska dotterbolag.[206]

Ett särskilt framträdande exempel är fraktföretaget A.P. Maersk med ett lokalt kontor i hamnstaden Odessa i södra Ukraina. Där hade den lokala avdelningschefen bett om undantag från säkerhetsrutiner för att få installera revisionsmjukvaran M.E.Doc. När NotPetya väl hade tagit sig in via M.E.Doc-installationen spred det sig sedan inom Maersks interna nätverk. Detta gav upphov till mycket stora störningar globalt i företagets IT-miljöer. Globalt är Maersk driftansvarig i 76 hamnar och äger nära 800 fartyg. Maersk utgör ungefär 20 procent av världens fraktkapacitet, med 574 kontor i 130 länder.[207] APM Terminals, ett dotterbolag till Maersk som hanterar logistiken i containerhamnar, drabbades av också av störningar i flera stora hamnar runt om i världen; blandat annat i Nhava Sheva i Mumbai, Rotterdam, Mobile, Elizabeth och Los Angeles.[208]

Källor inifrån Maersk uppger att vissa servrar fortfarande använde Windows 2000 när NotPetya slog till. All data lagrad på lokala arbetsstationer uppges ha gått förlorad. Datorer, interna digitala telefonsystem och elektroniskt kontrollerade dörrar och grindar var ur funktion efter att alla system stängts ner eller blivit infekterade. Det finns inga tecken på att datorer ombord på fartyg infekterades av NotPetya.[209]

[204] Greenberg, Andy. "The untold story of NotPetya, the most devastating cyberattack in history". *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].
[205] Cherepanov, Anton. "Analysis of Telebots's cunning backdoor". ESET, 2017-07-04. https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ [Hämtad: 2019-02-15].
[206] Polityuk, Pavel och Auchard, Erik. "Global cyber attack likely cover for malware installation in Ukraine: police official". *Reuters*, 2017-06-29. https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19K1WI [Hämtad: 2019-02-15].
[207] Greenberg, Andy. "The untold story of NotPetya, the most devastating cyberattack in history". *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].
[208] The Maritime Executive. "Maersk's Cargo Operations Hit Hard by Cyberattack". https://www.maritime-executive.com/article/maersks-cargo-operations-hit-hard-by-cyberattack#gs.iTipKYI [Hämtad: 2019-02-15].
[209] Greenberg, Andy. "The untold story of NotPetya, the most devastating cyberattack in history". *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

Land och sektor	Spridning	Konsekvens	Omfattning
Amerikansk hälso- och sjukvårdssektor	Två sjukhus hos Heritage Valley Health Systems,[210] kapacitet på cirka 500 sängar.	Störningar i två sjukhus och tillhörande kontor med maskininfektioner även i laboratorier och diagnostikkontor.	Åtminstone ett kirurgiskt ingrepp fick ställas in. Patienter fick omdirigeras till andra sjukhus.
	Princeton Community Hospital.[211]	Störningar i tillgänglighet hos framförallt äldre system.	Hela organisationens nätverk ersattes.
Amerikansk transportsektor	APM Terminals i Pier 400, största containerterminalen i hamnen i Los Angeles, California.[212]	Störningar i system för leveranser och godshantering.	Containerterminalen stängdes ner och inkommande trafik stoppades, enbart 10 % av ordinarie kapacitet transporterades under incidenten.[213]
	APM Terminals, hamnen i Elizabeth, New Jersey.	Störningar i system för leveranser och godshantering.	Verksamheten fick stängas ner för dagen.[214]
	APM Terminals, hamnen i New York, New York.	Störningar i system för leveranser och godshantering.	Verksamheten fick stängas ner för dagen.[215]
	APM Terminals, hamnen i Mobile, Alabama.	Störningar i system för leveranser och godshantering. Störningar rapporterades även i kommunikations-system och utrustning så som godsvågar.	Alternativa processer etablerades för att hantera tullning som annars var automatiserad. Även kunder som levererade till hamnen fick övergå till manuell leveranshantering.[216]

[210] Glaser, April. ”U.S hospitals have been hit by the global ransomware attack”. *Recode*, 2017-06-27. https://www.recode.net/2017/6/27/15881666/global-eu-cyber-attack-us-hackers-nsa-hospitals [Hämtad: 2019-03-27].

[211] Davis, Jessica. ”West Virigina hospital replaces computers after Petya cyberattack”. *Healthcare IT News*, 2017-06-30. https://www.healthcareitnews.com/news/west-virginia-hospital-replaces-computers-after-petya-cyberattack [Hämtad: 2019-03-29].

[212] Burnson, Patrick. ”Port of Los Angeles Reacts to Petya Crisis as CargoSmart Provids Some Supply Chain Solutions”. *Supply Chain Management Review*, 2017-06-28. http://www.scmr.com/article/port_of_los_angeles_reacts_to_pety_crisis_as_cargosmart_provides_some_suppl [Hämtad: 2019-03-29]; *CBS Los Angeles*. ”Global Cyberattack Shuts Down Port of LA’s Largest Terminal. https://losangeles.cbslocal.com/2017/06/27/cyberattack-port-of-la/

[213] Cristales, Denny. ”Homeland Security Committee examined LA Ports’ cyber protection and vulnerabilities at field hearing”. *Signal Tribune*, 2017-11-03. https://signaltribunenewspaper.com/35673/news/homeland-security-committee-examined-la-ports-cyber-protection-and-vulnerabilities-at-field-hearing/ [Hämtad: 2019-03-29].

[214] Greenberg, Andy. “The untold story of NotPetya, the most devastating cyberattack in history”. *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15]; Burnson, Patrick. ”Port of Los Angeles Reacts to Petya Crisis as CargoSmart Provids Some Supply Chain Solutions”. *Supply Chain Management Review*, 2017-06-28. http://www.scmr.com/article/port_of_los_angeles_reacts_to_pety_crisis_as_cargosmart_provides_some_suppl [Hämtad: 2019-03-29]

[215] Burnson, Patrick. ”Port of Los Angeles Reacts to Petya Crisis as CargoSmart Provids Some Supply Chain Solutions”. *Supply Chain Management Review*, 2017-06-28. http://www.scmr.com/article/port_of_los_angeles_reacts_to_pety_crisis_as_cargosmart_provides_some_suppl [Hämtad: 2019-03-29]

[216] Specker, Lawrence. ”’Petya’ cyberattack: Teamwork, pride fueled Alabama terminal’s fight to rebound”. *Advance Local*, 2017-07-09. https://www.al.com/news/index.ssf/2017/07/petya_cyberattack_teamwork_pri.html [Hämtad: 2019-03-28].

Indisk transportsektor[217]	APM Terminals Mumbai som står för nära 45 % av genomströmningen av containrar i Jawaharlal Nehru,[218] Indiens största containerhamn.[219]	Störningar i system för leveranser och godshantering.	Verksamheten fick återupptas manuellt efter att ha avstannat helt när systemet för godshantering slogs ut.
Nederländsk transportsektor	APM Terminals[220] i Rotterdam hamn, Europas största hamn.[221]	Störningar i system för leveranser och godshantering.	Företagets båda terminaler slogs ut.
	TNT Express.[222]	Störningar i administrativa system.	Förseningar i kundtjänst.
Rysk energisektor	Rosneft[223].	Servrar infekterade.	Användandet av reservkontrollsystem förhindrade inverkan på produktion.
Rysk banksektorn	Home Credit Lending.[224]	Administrativa system stängdes ner i preventivt syfte efter infektion.	Alla ryska kontor stängdes ner.

Trots övergången till manuella rutiner sjönk den hanterade volymen av transportgods med 20 procent.[225] Eftersom APM Terminals system blev påverkade kunde inte bokningsdata för containrarna hanteras. Maersk uppskattade att attacken hade orsakat mellan 250 och 300 miljoner US dollar i förluster och kostnader. [226] Maersk gav även sina kunder ersättning för kostnader som uppstått till följd av driftstörningarna.[227]

För att få igång verksamheten igen installerades 4000 nya servrar och 45 000 nya datorer under en period på tio dagar. För att snabba på processen anlitades närmare 200 konsulter från Deloitte. Under två månader arbetade dessa med att upprätta all systemfunktionalitet. Under inledningsfasen av arbetet fann personalen säkerhetskopior av nästan alla lokala servrar, men den enda domänkontrollantserver som inte infekterats befann sig i Ghana.

[217] IANS. ”Indian government has started taking measures to protect itself from the latest ransomware attack”. *First Post*, 2017-06-28. https://www.firstpost.com/tech/news-analysis/indian-government-has-started-taking-measures-to-protect-itself-from-the-latest-ransomware-attack-3835135.html [Hämtad: 2019-02-18].

[218] APM Terminals Mumbai. ”Welcome to APM Terminals Mumbai”. U.d. https://www.apmtmumbai.com/ [Hämtad: 2019-03-29].

[219] Jawaharlal Nehru Port. “The Birth of JNPT”. 2018-09-28. http://jnport.gov.in/ [Hämtad: 2019-03-29].

[220] Thomson, Iain. “Virus (cough, cough, Petya) goes postal at FedEx, shares halted”. *The Register*, 2018-06-28. https://www.theregister.co.uk/2017/06/28/fedex_tnt_express_virus_attack/ [Hämtad: 2019-02-18]; *Port of Rotterdam*. “More vessels call on a safe port”. 2018-01-15. https://www.portofrotterdam.com/en/news-and-press-releases/more-vessels-call-on-a-safe-port [Hämtad: 2019-02-18].

[221] Port of Rotterdam Authority. ”Facts and figures”. U.d. Tillgänglig via https://www.portofrotterdam.com/sites/default/files/facts-and-figures-port-of-rotterdam.pdf?token=CJ3nvKBO [Hämtad: 2019-03-29].

[222] FedEx. “FedEx Files 10-K with Additional Disclosure on Cyber-Attack Affecting TNT Express Systems”. 2017-07-17. http://investors.fedex.com/news-and-events/investor-news/news-release-details/2017/FedEx-Files-10-K-with-Additional-Disclosure-on-Cyber-Attack-Affecting-TNT-Express-Systems/default.aspx [Hämtad: 2019-03-29].

[223] *Offshore Energy Today*. “Maersk, Rosneft hit by cyberattack”. 2017-06-28. https://www.offshoreenergy-today.com/report-maersk-rosneft-hit-by-cyberattack/ [Hämtad: 2019-02-18].

[224] Zavyalova, Kira; Stubbs, Jack och Neely Jason. ”Home Credit’s Russian bank suspends IT systems after cyber attack”. *Reuters*, 2107-06-28. https://www.reuters.com/article/us-cyber-attack-homecredit-russia/home-credits-russian-bank-suspends-it-systems-after-cyber-attack-idUSKBN19J10I [Hämtad: 2019-03-29].

[225] Chirgwin, Richard. “IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz”. *The Register*, 2018-01-25. https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/ [Hämtad: 2019-02-15].

[226] *2017 Annual Report*. A.P. Møller- Mærsk A/S, 2017, s. 54. https://investor.maersk.com/static-files/5d68faa5-f869-4c08-8a1d-9660fe889360 [Hämtad: 2019-04-08].

[227] Greenberg, Andy. “The untold story of NotPetya, the most devastating cyberattack in history”. *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

Den hade klarat sig från att infekteras tack vare ett lokalt strömavbrott och var då inte tillgänglig under utbrottet. Denna domänkontrollantserver var central för återskapandet av systemfunktionaliteten då den innehöll nödvändig information om användarna och rättigheterna i Maersks IT-miljöer.[228]

3.2.1 Ukraina

En absolut majoritet av de organisationer som drabbades av NotPetya fanns i Ukraina. Totalt uppskattas mellan 60 och 80 procent av kryptomasken globala spridning utgjorts av aktörer verksamma i Ukraina. Orsaken till detta är att en stor del av det ukrainska näringslivet använder M.E.Doc, medan programvaran har få användare utanför landet.[229] En senior ukrainsk regeringstjänsteman uppskattade att 10 procent av alla datorer i landet förstördes av NotPetya.[230]

Tabell 9. NotPetyas spridning och konsekvenser i NIS-sektorer i Ukraina.

Sektor	Spridning	Konsekvens
Banksektor	Oschadbank, Sberbank, Ukrsotsbank, Ukrgasbank, OTP Bank och PrivatBank.	Tillgänglighetsstörningar i framför allt bankautomater, kortbetalningssystem, vissa administrativa system samt webbsidor.
Hälso- och sjukvårdssektor	Fyra stora sjukhus, Boriskliniken (Kievs största).	Boris-kliniken drabbades av störningar i alla system utom medicinteknisk utrustning, inklusive journalsystem.
Energisektor	Statliga Ukrenergo, Kyivenergo (Kievs största elproducent).	Administrativa system slogs ut.
Transportsektor	Boryspil International Airport, Kharkivs internationella flygplats, Kievs tunnelbana.	Lindriga förseningar i flygtrafiken. Kortbetalningar inte möjliga i tunnelbanan.
Offentlig sektor	Energiministeriet, finansministeriet, kulturministeriet, inrikesministeriet, ministerrådet, den nationella polisen, ukrainska regeringen	Webbsidor otillgängliga samt vissa administrativa system nere. Inga bestående förluster av data rapporterades.

Enligt ett uttalande av Ukrainas infrastrukturminister drabbades i princip alla federala myndigheter, minst fyra av Kievs sjukhus, sex elbolag, minst 22 ukrainska banker och bankautomater samt kortbetalningssystem hos återförsäljare och transport.[231] Incidenter och störningar har bland annat identifierats i banksektorn, sjukvårdssektorn, energisektorn och transportsektorn och inom offentlig verksamhet. Likt i fallet WannaCry bedöms en ut-

[228] Greenberg, Andy. "The untold story of NotPetya, the most devastating cyberattack in history". *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

[229] Hern, Alex. "Ransomware attack 'not designed to make money', researchers claim". *The Guardian*, 2017-06-28. https://www.theguardian.com/technology/2017/jun/28/notpetya-ransomware-attack-ukraine-russia [Hämtad: 2019-02-15]; Wakefield, Jane. "Tax software blamed for cyber-attack spread". *BBC*, 2017-06-28. https://www.bbc.com/news/technology-40428967 [Hämtad: 2019-02-15].

[230] Greenberg, Andy. "The untold story of NotPetya, the most devastating cyberattack in history". *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

[231] Greenberg, Andy. "The untold story of NotPetya, the most devastating cyberattack in history". *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

bredd användning av icke-licenserade Windowsprodukter som inte kan installera säkerhetuppdateringar bidragit till kryptomaskens framfart, troligtvis även hos regeringen och försvarsministeriet.[232]

3.2.1.1 Konsekvenser i den ukrainska banksektorn

Statligt ägda Oschadbank, en av de största bankerna i landet[233], rapporterade att ungefär 90 procent av alla datorer på dess huvudkontor i Kiev låstes morgonen den 27 juni[234], den första dagen som NotPetya spreds. De meddelade att ingen kunddata hade äventyrats under störningen.[235] Kontantautomater runt om i Ukraina rapporteras också ha slagits ut,[236] bland annat hos just Oschadbank.[237] Anställda på Oschadbank menade att det tog banken en vecka för verksamheten att återhämta sig.[238]Att banker drabbades innebar även att betaltjänster på bensinstationer och i dagligvarubutiker slogs ut, vilket skapade oro för hur länge kontanter skulle räcka till för att köpa mat och andra viktiga förnödenheter.[239] Hemsidorna tillhörande Oschadbank, Sberbank, Ukrsotsbank, Ukrgasbank, OTP Bank och PrivatBank låg också nere till följd av attacken.[240] Den Ukrainska centralbanken gick under attacken ut med en uppmaning till bank- och finansmarknaden, i vilken de manade till försiktighet vad gäller öppnande av mejl som kunde innehålla skadlig kod, en åtgärd som i relation till situationen kan framstå som irrelevant eftersom NotPetya inte spreds via mejl.[241]

3.2.1.2 Konsekvenser i den ukrainska hälso- och sjukvårdssektorn

I ukrainska hälso- och sjukvårdssektorn drabbades fyra stora sjukhus och hos den största medicinska kliniken i Kiev, Boris-kliniken, infekterades alla datorer förutom de som användes i medicinteknisk utrustning. Eftersom infektionen påverkade klinikens journalsystem bröt kliniken indirekt mot ukrainsk lag som statuerar att all patientinformation ska sparas i 25 år. Informationsförlusten förminskades dock av att det fanns säkerhetskopior av viktig data och att personalen övergick till att arbeta manuellt med papper och penna.[242]

---

[232] Goncharova, Olena; Grytsenko, Oksana och Krasnikov, Denys. ”Ukraine finds itself at the epicenter of global cyberattack. *Kyiv Post,* 2017-06-30. https://www.pressreader.com/ukraine/kyiv-post/20170630/281741269437161 [Hämtad: 2019-02-15].

[233] Dearden, Lizzie. “Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers“.*The Independent,* 2017-06-27. https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html [Hämtad: 2019-02-15]

[234] Greenberg, Andy. “The untold story of NotPetya, the most devastating cyberattack in history”. *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

[235] Dearden, Lizzie. “Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers“.*The Independent,* 2017-06-27. https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html [Hämtad: 2019-02-15].

[236] Ibid.

[237] Zinets, Natalia. ”Ukraine central bank warns of new cyber-attack risk”. *Reuters,* 2017-08-18. https://www.reuters.com/article/us-cyber-ukraine-banking-idUSKCN1AY0Y4 [Hämtad: 2019-03-27].

[238]Satter, Raphael. ”Official: firm at center of cyberattack knew of problems”. *Associated Press.* https://apnews.com/8b02768224de485eb4e7b33ae55b02f2 [Hämtad: 2019-02-15].

[239] Greenberg, Andy. “The untold story of NotPetya, the most devastating cyberattack in history”. *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

[240] *Ukrinform*. ”Cyber attack on Ukrainian government and corporate networks halted”. 2017-06-28. https://www.ukrinform.net/rubric-polytics/2255698-cyber-attack-on-ukrainian-government-and-corporate-networks-halted.html [Hämtad: 2019-02-15].

[241] National Bank of Ukraine. “The National Bank of Ukraine Warned Banks and other Financial Market Participants about an External Hacker Attack”. 2017-06-27. https://bank.gov.ua/control/en/publish/article?art_id=51024813 [Hämtad: 2019-02-15].

[242] Borys, Christian. “Ukraine braces for further cyber-attacks”. *BBC,* 2017-07-26. https://www.bbc.com/news/technology-40706093 [Hämtad: 2019-02-15].

3.2.1.3 Konsekvenser i den ukrainska energisektorn

I ukrainska energisektorn drabbades ett flertal organisationer av NotPetya. Statliga Ukrenergo, som är ansvariga för elnätet som levererar elektriciteten till en majoritet av Kievs elkonsumenter. Ukrenergos hemsida låg nere till följd av infektionen[243]. Inga störningar i elförsörjningen rapporterades men ett antal datorer fick kopplas bort från nätverket[244]

Kievs största elproducent Kyivenergo rapporterade också att de blivit drabbade och därför behövt stänga av datorer, men menade tidigt att situationen var under kontroll.[245] Inga störningar rapporterades heller i leveransen av el.

Vidare slogs den automatiska radioaktivitetsmätningen i Tjernobyl-zonen ut, varför man fick gå över till manuella rutiner för att kunna fortsätta mäta.[246]

3.2.1.4 Konsekvenser i den ukrainska transportsektorn

Inom transportsektorn drabbades exempelvis Boryspil International Aiport. På flygplatsen, som är Ukrainas största, slogs både datorer och ankomsttavlor ut. Störningarna i verksamhet och flygtrafik beskrivs som lindriga. Nyhetsmedia rapporterade under NotPetyas första dag att vissa förseningar var möjliga.[247]

Kharkivs internationella flygplats övergick till manuella rutiner för incheckning, men rapporterade inga andra störningar.[248] Även Kievs tunnelbana påverkades av NotPetya, med effekten att det inte gick att betala för biljetter med bankkort.[249] Vad gäller driften av tågen rapporteras dock inga störningar.

3.2.1.5 Konsekvenser i den ukrainska offentlig sektorn

Inom den offentliga sektorn slogs hemsidorna för energiministeriet, finansministeriet, kulturministeriet, inrikesministeriet, ministerrådet, den nationella polisen och den ukrainska regeringen drabbades också.[250] Ukrainas vice premiärminister berättade i sociala medier att regeringens nätverk låg nere, och infrastrukturministern menade att regeringen blev lamslagen till följd av störningarna[251].

---

[243] Brewster, Thomas. "Another Massive Ransomware Outbreak Is Going Global Fast". *Forbes*, 2017-06-27. https://www.forbes.com/sites/thomasbrewster/2017/06/27/ransomware-spreads-rapidly-hitting-power-companies-banks-airlines-metro/#62ae1fb27abd [Hämtad: 2019-03-27].

[244] Interfax-Ukraine. "Kyivenergo hacked, Ukrenergo affected". *Kyiv Post*, 2017-06-27. https://www.kyivpost.com/ukraine-politics/kyivenergo-hacked-ukrenergo-affected.html?cn-reloaded=1 [Hämtad: 2019-02-15]; Chornokondratenko, Margaryta. "Ukraine power company says was hit by second cyber attack". *Reuters*, 2017-06-30. https://www.reuters.com/article/uk-cyber-attack-ukrenergo/ukraine-power-company-says-was-hit-by-second-cyber-attack-idUKKBN19L0OM [Hämtad: 2019-02-15].

[245] Interfax-Ukraine. "Kyivenergo hacked, Ukrenergo affected". *Kyiv Post*, 2017-06-27. https://www.kyivpost.com/ukraine-politics/kyivenergo-hacked-ukrenergo-affected.html [Hämtad: 2019-02-15].

[246] Curtis, Sophie. "Chernobyl nuclear power plant hit by 'Petya' ransomware attack causing havoc across the globe". *Daily Mirror*, 2017-06-27. https://www.mirror.co.uk/tech/chernobyl-nuclear-power-plant-hit-10697960 [Hämtad: 2019-02-15].

[247] Polityuk, Pavel; Prentice, Alessandra och Pomeroy, Robin. "Kiev airport hit by cyber attack, delays possible". *Reuters*, 2017-06-27. https://www.reuters.com/article/us-cyber-attack-ukraine-airport/kiev-airport-hit-by-cyber-attack-delays-possible-idUSKBN19I1OR?il=0 [Hämtad: 2019-02-15].

[248] Kharkiv Airport. " Уважаемые пассажиры!". Facebook, 2017-06-27, [Översatt med Google Översätt]. https://www.facebook.com/hrk.aero/posts/1533337316697274:0 [Hämtad: 2019-04-01].

[249] Perlroth, Nicole; Scott, Mark och Frenkel, Sheera. "Cyberattack Hits Ukraine Then Spreads Internationally". *New York Times*, 2017-06-27. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html [Hämtad: 2019-03-27].

[250] *Censor.net*. "List of Ukrainian companies and agencies whose websites were attacked by hackers on June 27 (live updates)". 2017-06-27. https://en.censor.net.ua/n445650 [Hämtad: 2019-02-15]; GroupIB. "Petya starts with Ukraine and then goes global". 2017-06-27. https://www.group-ib.com/blog/petya. [Hämtad: 2019-03-27].

[251] Dearden, Lizzie. "Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers".*The Independent*, 2017-06-27. https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html [Hämtad: 2019-02-15]; Greenberg, Andy. "The untold story of NotPetya, the most devastating cyberattack in history". *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

3.2.2 Sverige

Tabell 10. NotPetyas spridning och konsekvenser i Sverige.

Sektor	Spridning	Konsekvens
Transportsektorn	APM Terminals i Göteborgs hamn. [252]	Störningar i system för leveranser och hanterande av gods. Verksamheten fick avslutas då systemen var utslagna. Containrar gick inte att hämta ut. Incidenten sammanföll med pågående strejk i hamnen, vilket vidare reducerade hanteringsförmågan. [253]

I Sverige verkar enbart transportsektorn ha drabbats av NotPetya. Det tydligaste exemplet är containerhamnen i Göteborg, vilken drabbades eftersom driften av terminalsystemet för hamnlogistik sköttes av företaget APM Terminals, vilka var ett offer för NotPetya.[254] NotPetya sammanföll med redan existerande verksamhetsstörning till följd av en pågående strejk.

Till följd av störningarna fick APM Terminals övergå till manuell inventering av containrar. Gods från fartyg och järnväg prioriterades, samtidigt som all hantering av gods från lastbilstrafik stoppades. Kontroller gjordes även på containrar som innehöll farligt gods.[255] Speditionsbolaget Swedebridge uppgav att knappt något gods ankom hamnen på grund av strejken och att det lilla som faktiskt kommit in inte gick att hämta ut på grund av att IT-systemen låg nere. Swedebridge menade att störningarna potentiellt skulle kunna leda till att vissa av hamnens kunder riskerade konkurs.[256]

CERT-SE publicerade den 27:e juni en varning i vilken Service Message Block-protokollet identifierades som en potentiell spridningsväg för NotPetya.[257] I revisionen av meddelandet, daterad den 28 juni, uppmanade CERT-SE till uppdatering av mjukvara, virusskydd och operativsystem, samt att genom övning säkerställa att rutiner för säkerhetskopiering och återställning fungerar. CERT-SE refererade även till en mer detaljerad rapport från CERT-EU, [258] vilken konstaterade att nya infektioner vid det laget inte längre var troliga, men att framgångsrika angreppsmetoder sannolikt återanvänds i framtiden. Därför uppmuntrades säkerhetsuppdateringar, säkerhetsrutiner som förhindrar höjandet av användarprivilegier, begränsande av kommunikationen mellan datorer i det lokala nätverket samt att inte återanvända administratorslösenord i flera system.[259]

[252] Tenitskaja, Alexandra Carlsson och Dickson, Staffan. ”Storföretag drabbade av nätattack”. *Aftonbladet*, 2017-06-27. https://www.aftonbladet.se/nyheter/a/Ja618/hackerattack-mot-goteborgs-hamn [Hämtad: 2019-02-18].

[253] TT / NyTeknik. ”Göteborgs hamn svårt drabbad av it-attack”. *Ny Teknik*, 2017-06-28. https://www.nyteknik.se/digitalisering/goteborgs-hamn-svart-drabbad-av-it-attack-6858639 [Hämtad: 2019-02-18].

[254] Tenitskaja, Alexandra Carlsson och Dickson, Staffan. ”Storföretag drabbade av nätattack”. *Aftonbladet*, 2017-06-27. https://www.aftonbladet.se/nyheter/a/Ja618/hackerattack-mot-goteborgs-hamn [Hämtad: 2019-02-18].

[255] TT. ”Göteborgs hamn lamslagen av IT-attacken”. *Svenska Dagbladet*, 2017-06-28. https://www.svd.se/oklart-hur-virusattack-drabbar-sverige [Hämtad: 2019-02-18].

[256] TT / NyTeknik. ”Göteborgs hamn svårt drabbad av it-attack”. *Ny Teknik*, 2017-06-28. https://www.nyteknik.se/digitalisering/goteborgs-hamn-svart-drabbad-av-it-attack-6858639 [Hämtad: 2019-02-18].

[257] CERT-SE. ”Nytt angrepp av utpressningsprogram”. 2017-06-27. [Arkiverad] https://web.archive.org/web/20170627171605/https://www.cert.se/2017/06/nytt-angrepp-av-utpressningsprogram [Hämtad: 2019-02-18].

[258] CERT-SE. ”Nytt angrepp av utpressningsprogram”. 2017-06-29. https://www.cert.se/2017/06/nytt-angrepp-av-utpressningsprogram [Hämtad: 2019-02-18].

[259] CERT-EU. ”CERT-EU Security Advisory 2017-014 Petya-Like Malware Campaign“. 2017-06-29. https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-014.pdf [Hämtad: 2019-02-18].

4 Analys av förutsättningar för att hantera kryptomaskar

Detta kapitel svarar på rapportens andra fråga; vad krävs för att organisationer ska kunna förebygga och hantera kryptomaskar? Analysen baseras på det redovisade materialet i kapitlen ovan. Utöver analysen av vilka generella förutsättningar som krävs gör kapitlet även kopplingar till förutsättningar i den svenska kontexten.

4.1 Cyberhygien

Från rapporteringen om vilka åtgärder eller faktorer som förebyggde, eller begränsade verkningarna av kryptomaskarna syns att cyberhygien var en viktig faktor. Det saknas en vedertagen definition för vad cyberhygien är, men det anses ofta vara grundläggande och relativt enkla vardagsrutiner för att öka cybersäkerheten.[260] Förslag på konkreta åtgärder som bör ingå i arbetet är att:

- identifiera av tillgångar som bör prioriteras i säkerhetsarbetet[261]
- identifiera och hantera säkerhetsrisker mot dessa prioriterade tillgångar [262]
- etablera perimeterskydd för faciliteter, nätverk, individer, med mera[263]
- skapa försvar på djupet genom flera lager av säkerhetskontroller.[264]
- etablera en incidenthanteringsplan[265]
- öka medvetenheten om hot och åtgärder[266]
- hantera och övervaka nätverkstrafik och dataflöden med mera[267]

[260] *Review of Cyber Hygiene practices*. ENISA, 2016. DOI 10.2824/352617. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport [Hämtad: 2019-03-27]; Lewis, James Andrew. *Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage*. Washington: Center for Strategic & International Studies, 2014. http://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140313_FireEye_WhitePaper_Final.pdf [Hämtad: 2019-03-27]; Trevors, Matthew. ”Cyber Hygiene: 11 Essential Practices”. *Insider Threat Blog*, Carnegie Mellon University, 2017-11-15. https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html [Hämtad: 2019-03-27].

[261] *Review of Cyber Hygiene practices*. ENISA, 2016. DOI 10.2824/352617. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport [Hämtad: 2019-03-27]; Trevors, Matthew. ”Cyber Hygiene: 11 Essential Practices”. *Insider Threat Blog*, Carnegie Mellon University, 2017-11-15. https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html [Hämtad: 2019-03-27].

[262] Ibid.

[263] *Review of Cyber Hygiene practices*. ENISA, 2016. DOI 10.2824/352617. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport [Hämtad: 2019-03-27]; Lewis, James Andrew. *Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage*. Washington: Center for Strategic & International Studies, 2014. http://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140313_FireEye_WhitePaper_Final.pdf [Hämtad: 2019-03-27].

[264] Ibid.

[265] *Review of Cyber Hygiene practices*. ENISA, 2016. DOI 10.2824/352617. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport [Hämtad: 2019-03-27]; Trevors, Matthew. ”Cyber Hygiene: 11 Essential Practices”. *Insider Threat Blog*, Carnegie Mellon University, 2017-11-15. https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html [Hämtad: 2019-03-27]

[266] *Review of Cyber Hygiene practices*. ENISA, 2016. DOI 10.2824/352617. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport [Hämtad: 2019-03-27]; Lewis, James Andrew. *Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage*. Washington: Center for Strategic & International Studies, 2014. http://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140313_FireEye_WhitePaper_Final.pdf [Hämtad: 2019-03-27]; Trevors, Matthew. ”Cyber Hygiene: 11 Essential Practices”. *Insider Threat Blog*, Carnegie Mellon University, 2017-11-15. https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html [Hämtad: 2019-03-27]

[267] *Review of Cyber Hygiene practices*. ENISA, 2016. DOI 10.2824/352617. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport [Hämtad: 2019-03-27]; Trevors, Matthew. ”Cyber Hygiene: 11

- begränsa internkommunikation mellan system i nätverket.[268]
- genomföra säkerhetsuppdateringar i mjukvara[269]
- genomföra säkerhetskopiering av viktiga informationstillgångar.[270]

De åtgärder som tydligast identifierats i rapporteringen innefattar att identifiera tillgångar och risker, etablera en incidenthanteringsplan, öka medvetenheten om hot och åtgärder, genomföra säkerhetsuppdateringar, kontinuerlig säkerhetskopiering av viktig information, skapandet av ett försvar på djupet samt att begränsa internkommunikationen mellan system i nätverket.

4.1.1 Identifiera tillgångar och risker

För ett effektivt riskhanteringsarbete måste tillgångar och risker identifieras så att förebyggande åtgärder kan vidtas. Situationen hos Timrå kommun och brittiska NHS visade på risker som kan uppstå när ansvaret för säkerhet i nätverks- och informationssystem utkontrakteras. Effektiv riskhantering kräver god information så att korrekta bedömningar kan göras av den aktör som ansvarar för säkerheten. Timrå kommun fick exempelvis information om att leverantören planerade att uppdatera kommunens system, en uppdatering som ställdes in. Därför var kommunen fortfarande sårbar vid WannaCrys utbrott. Källmaterialet visade att parterna under hösten 2017 var involverade i en rättslig tvist om ansvarsförhållandet.[271] I den kinesiska banksektorn fanns exempel på att ansvariga myndigheter beordrade bank- och finansaktörer att själva inventera sin nätverkssäkerhet och se över rutiner för riskhantering, för att på så sätt stävja vidare spridning av WannaCry.[272]

I Sverige måste leverantörer för samhällsviktiga tjänster enligt lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster genomföra en riskanalys. Leverantörer av samhällsviktiga tjänster måste dessutom ha en dokumenterad klassning av informationstillgångar (enligt behov av konfidentialitet, riktighet och integritet) samt identifiera och värdera risker för information, nätverk och system.[273] MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster rekommenderar även att ansvar för säkerhetsåtgärderna hanteras i avtal vid utkontraktering.[274]

Essential Practices". *Insider Threat Blog*, Carnegie Mellon University, 2017-11-15. https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html [Hämtad: 2019-03-27]

[268] *Review of Cyber Hygiene practices*. ENISA, 2016. DOI 10.2824/352617. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport [Hämtad: 2019-03-27]; Lewis, James Andrew. *Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage*. Washington: Center for Strategic & International Studies, 2014. http://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140313_FireEye_WhitePaper_Final.pdf [Hämtad: 2019-03-27].

[269] *Review of Cyber Hygiene practices*. ENISA, 2016. DOI 10.2824/352617. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport [Hämtad: 2019-03-27]; Lewis, James Andrew. *Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage*. Washington: Center for Strategic & International Studies, 2014. http://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140313_FireEye_WhitePaper_Final.pdf [Hämtad: 2019-03-27]; Trevors, Matthew. "Cyber Hygiene: 11 Essential Practices". *Insider Threat Blog*, Carnegie Mellon University, 2017-11-15. https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html [Hämtad: 2019-03-27]

[270] *Review of Cyber Hygiene practices*. ENISA, 2016. DOI 10.2824/352617. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport [Hämtad: 2019-03-27].

[271] Lindblom, Hans. "Timrå kommun hade gammalt virusskydd". *SVT*, 2017-10-29. https://www.svt.se/nyheter/lokalt/vasternorrland/timra-kommun-hade-gammalt-virusskydd [Hämtad: 2019-02-14].

[272] Hersey, Frank. "Here's what we know about how WannaCry has affected China". *TechNode*, 2017-05-15. https://technode.com/2017/05/15/how-hard-did-wannacry-virus-hit-china/ [Hämtad: 2019-02-05].

[273] MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. 8§. https://www.msb.se/externdata/rs/9b5c0905-20c5-4fe6-8341-5b481cc570a4.pdf [Hämtad: 2019-03-26]

[274] Ibid.

4.1.2 Effektiv incidenthantering

I den tyska transportsektorn ska en av de försvårande faktorerna i hanteringen av WannaCry varit avsaknaden av en incidenthanteringsplan och av dedikerade resurser för att genomföra en sådan plan.[275] Med en tydligare incidenthanteringsplan hade det varit mer sannolikt att infekterade system hade kunnat avskärmas och därmed begränsa spridningen.[276] Även om en incidenthanteringsplan fanns för NHS i brittiska sjukvårdssektorn tyder utredningar på att den varken var känd eller tillämpades inom flera delar av organisationen. Fallet NHS visar även hur ansvarsroller för incidenthantering och ledning vid incidenter blir otydliga utan en förankrad incidenthanteringsplan.[277] Detta visar på vikten av att höja anställdas medvetenhet kring säkerhetsfrågor samt hur de bör agera då störningar uppstår i organisationen till följd av IT-incidenter.

Enligt NIS-direktivet ska de europeiska medlemsstaterna upprätta nationella informations- och cybersäkerhetsstrategier som innefattar riskbedömningsplaner för samhällsviktig verksamhet.[278] I Sverige måste leverantörer för samhällsviktiga tjänster upprätta en åtgärdsplan för riskerna enligt lag (2018:1174). MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster[279] fastställer även att åtgärdsplanerna bör klargöra en prioritering där åtgärder kopplas till skyddsnivåer och konsekvensnivåer för risker, samt klargöra vart ansvaret för ledning och tillämpning av åtgärder ligger.

4.1.3 Medvetenhet

Konsekvenserna av de två kryptomaskarna belyser vikten av grundläggande cyberhygien för att skydda organisationer mot incidenter i nätverks- och informationssystem. När incidenter ändå inträffar i verksamhetskritiska system är det viktigt att planering för upprätthållande av verksamhetskontinuiteten finns och att alternativa rutiner tagits fram och övats med berörd personal som en del av det arbetet. Som NHS utvärdering av WannaCry visade fanns tendens till att mer cybermogna lokala organisationer hörsammade rekommendationer från central nivå än vad mindre mogna organisationer gjorde. [280]

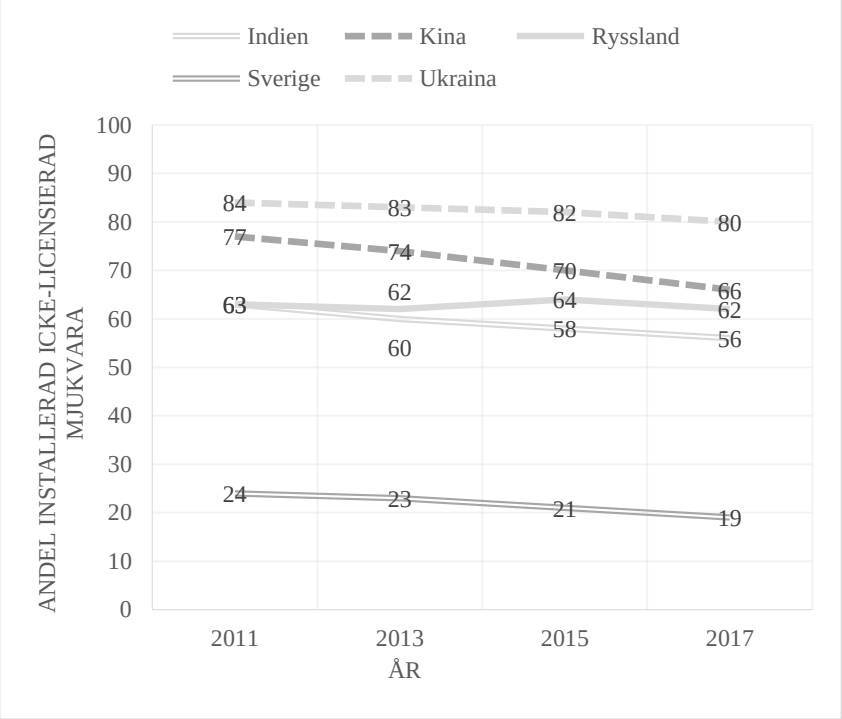
På nationell nivå i Europa är det enheterna för hantering av IT-säkerhetsincidenter (Computer Security Incident Response Team, CSIRT) som ska främja övningar för cybersäkerhet i samhällsviktig verksamhet, bland annat via den europeiska samarbetsgruppen.[281] Mycket av den nationella utbildnings- och övningsverksamhet inom cybersäkerhet som bedrivs i Sverige ansvarar MSB för,[282] som även tillhandahåller Sveriges nationella CSIRT – CERT-SE. Även om nationella och multinationella plattformar för övning är en viktig mekanism för att öka medvetenheten och kompetensen att hantera incidenter, påvisar fallen WannaCry och NotPetya att utbildning även måste tillåta att leverantörer tränar

[275] Van Gompel, Marieke. ”WannaCry virus was ‘wake-up call’ for railway industry”. *RailTech.com*, 2017-12-11. https://www.railtech.com/all/2017/12/11/wannacry-virus-was-wake-up-call-for-railway-industry/ [Hämtad: 2019-02-14].
[276] Ibid.
[277] *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017., s. 9. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].
[278] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen EUT L 194, 19.7.2016, Artikel 7.
[279] MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster, s. 9. https://www.msb.se/externdata/rs/9b5c0905-20c5-4fe6-8341-5b481cc570a4.pdf [Hämtad: 2019-03-26].
[280] *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].
[281] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen EUT L 194, 19.7.2016, Artikel 8, 11, 12.
[282] *Samlad informations och cybersäkerhetshandlingsplan för åren 2019–2022*. Myndigheten för samhällsskydd och beredskap, 2019-03-01. ISBN 978-91-7383-918-1, https://www.msb.se/RibData/Filer/pdf/28804.pdf [Hämdatum: 2019-03-26].

på utförandet av sina egna incidenthanteringsplaner. MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster fastställer att övningar av interna roller och ansvar ska genomföras.[283]

4.1.4 Säkerhetsuppdateringar

I flera länder infekterades nätverks- och informationssystem på grund av att operativsystem saknat nödvändiga säkerhetsuppdateringar. För det första rörde det sig om utdaterade operativsystem som inte längre stöddes med säkerhetsuppdateringar, så som Russian Post som fortfarande använde Windows XP vid WannaCrys utbrott.[284] Även i Indien pekade experter på att det utbredda användandet av Windows XP gjort landet sårbart.[285] För det andra angav flera källor användandet av icke-licensierade operativsystem, där säkerhetsuppdateringar inte kan installeras, som en viktig faktor.



Figur 1. Fördelning av andelen icke-licensierad mjukvara. Källa: The Software Alliance.[286]

[283] MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. https://www.msb.se/externdata/rs/9b5c0905-20c5-4fe6-8341-5b481cc570a4.pdf [Hämtad: 2019-03-26].

[284] Moore-Colyer, Roland. "WannaCry Wallops Russian Post, Highlightning The Risk Of Legacy IT". *Silicon*, 2017-05-25. https://www.silicon.co.uk/security/wannacry-russian-post-213099 [Hämtad: 2019-03-27].

[285] *Indian Express*. "WannaCry ransomware: Computers at West Bengal State electricity firm hit". 2017-05-15. https://indianexpress.com/article/technology/tech-news-technology/wannacry-ransomware-computers-at-west-bengal-state-electricity-firm-hit/ [Hämtad: 2019-02-05].

[286] *Software Management: Security Imperative, Business Opportunity*. The Software Alliance, 2018. https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf [Hämtad: 2019-04-01].

I Indien,[287] Kina,[288] Ryssland[289] och Ukraina[290] lyftes just icke-licensierad programvara fram som ett säkerhetsproblem. Även om statistiken från The Software Alliance inte visar fördelningen av icke-licensierad mjukvara för enskilda sektorer, ger det en generell bild av hur många system som kan förväntas vara sårbara. Användningen av icke-licensierad mjukvara är högre i länderna där problematiken lyfts i materialet (se Figur 1) än exempelvis i Sverige.[291] Denna rapports material visade också att få svenska organisationer drabbades av WannaCry, och vid en infektion fick det inte någon betydande inverkan på deras primära tjänsteleveranser. Både användandet av icke-licensierad och föråldrad mjukvara kan vara tecken på en bristfällig säkerhetskultur där arbetet med att säkra system inte prioriteras.

En viktig aspekt att beakta är att inte alla system kan uppdateras. NHS pekade exempelvis på att äldre medicintekniska system med inbäddad mjukvara i vissa fall inte kunde uppdateras alls.[292] I andra fall kunde systemen uppdateras, men då endast av tillverkaren. Även när det var tekniskt möjligt att säkerhetsuppdatera system, krävdes stor försiktighet för att säkerställa att systemet fortfarande var kompatibelt med andra medicinska system. En lösning är att isolera dessa system, men det är oklart om några sådana försök gjordes.

Det bör poängteras att NotPetya hade förmåga att spridas internt i ett nätverk till system med korrekt utförda säkerhetsuppdateringar. I fallet Maersk krävdes enbart en installation av M.E.Doc på ett lokalt ukrainskt kontor för global spridning i Maersks system. Detta påvisar att säkerhetsuppdatering inte är en universallösning, även om flera länder identifierat dem som en viktig säkerhetsåtgärd. Risken är att de kritiska system som har blivit bedömda att vara skyddade ändå är sårbara genom andra infektionsvektorer.

4.2 Verksamhetskontinuitet

Som synes i exempelvis fallet Maersk finns ingen garanti för att uppdaterade verksamhetskritiska system inte infekteras av ett sofistikerat hot som NotPetya. Maersk och APM Terminals visar hur brister i kontinuitetsplanering och reservrutiner ledde till att personalen satt utan arbetsuppgifter då systemen slogs ut av NotPetya.[293] Detta föranleder en diskussion om vad som krävs för att säkerställa verksamhetens kontinuitet när en incident leder till störningar. I Sverige ska samhällsviktiga leverantörer identifiera behovet av kontinuitet i tjänsteleverans och bör etablera interna regler för att säkerställa kontinuitet, exempelvis accepterad återställandetid, alternativa arbetssätt och behov av uthållighet.[294]

---

[287] Das, Lalit. ”The advisory for Ransomware Threat-’WannaCry’”. Government of Odisha Home Department. http://www.homeodisha.gov.in/sites/default/files/AddFiles/WANNACRY.pdf [Hämtad: 2019-03-27].

[288] Richter, Wolf. “China's use of pirated software left it vulnerable to the WannaCry ransomware attack”. *Business Insider*, 2017-05-16. https://www.businessinsider.com/wannacry-ransomware-attack-china-2017-5?r=US&IR=T&IR=T [Hämtad: 2019-02-05]

[289] Kottasová, Ivana. ”Why Russia's cyber defenses are so weak”. *CNN*, 2015-05-15. https://money.cnn.com/2017/05/15/technology/russia-vulnerable-cyberattack/index.html [Hämtad: 2019-02-06].

[290] Goncharova, Olena; Grytsenko, Oksana och Krasnikov, Denys. ”Ukraine finds itself at the epicenter of global cyberattack. *Kyiv Post*, 2017-06-30. https://www.pressreader.com/ukraine/kyiv-post/20170630/281741269437161 [Hämtad: 2019-02-15].

[291] *Software Management: Security Imperative, Business Opportunity*. The Software Alliance, 2018. https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf [Hämtad: 2019-04-01].

[292] *Investigation: WannaCry cyber attack and the NHS*. London: National Audit Office, 2017.. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14]

[293] Greenberg, Andy. “The untold story of NotPetya, the most devastating cyberattack in history”. *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

[294] MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. https://www.msb.se/externdata/rs/9b5c0905-20c5-4fe6-8341-5b481cc570a4.pdf [Hämtad: 2019-03-26].

4.2.1 Etablera alternativa arbetssätt

Maersks hantering av NotPetya påvisade att alternativa rutiner behövdes utformas. Under incidenten blev företaget tvungna att göra detta ad hoc efter att alla system slagits ut, vilket var både tidskrävande och kostsamt. Övergången till manuella rutiner hos APM Terminals i Alabama innebar att även kunder och partners fick övergå till att arbeta manuellt.[295] En slutsats som kan dras är att organisationer bör se över sina reservrutiner. Genom att använda tjänster som WhatsApp kunde de anställda i flera delar av Maersk och APM Terminals kommunicera internt samt med kunder för att hantera verksamheten,[296] ett exempel på när nya tillfälliga rutiner uppstår ad hoc. Att upprätta alternativa rutiner ad hoc kan dock vara problematiskt, bland annat då arbetsrutiner utan genomförd riskanalys kan vara sårbara och medföra negativ inverkan på informationssäkerhet.

I Ukraina hade Kharkiv International Airport förmågan att övergå från elektroniska till manuella rutiner för incheckning när NotPetya slog till.[297] När det gäller WannaCry-incidenten övergick den indiska polismyndigheten till manuella metoder för att spara rapporter och andra dokument.[298] För den indiska polismyndigheten är det inte entydigt om det var ett medvetet och proaktivt förfarande eller om det rör sig om en strukturell fråga där rapporthantering skedde på papper till följd av myndigheten ej genomgått en digitalisering.

Dessa två fall är exempel där alternativa arbetssätt skapade högre resiliens för verksamheten, då verksamheten uppges ha fortlöpt utan kraftiga störningar i tjänsteleveransen trots pågående incident.

4.3 Informationsdelning och transparens

Både WannaCrys och NotPetyas spridning och verkningar belyste i flera fall transparens och informationsdelning som viktiga förutsättningar för incidenthanteringen. Dels handlade detta om korrekt och effektiv incidentrapportering, dels om myndigheters roll i kriskommunikation och rådgivning om incidenthantering.

4.3.1 Effektivt incidentrapporteringssystem

Generellt sett är det svårt att få fram jämförbar och konkret information om kryptomaskarnas spridning och i synnerhet om påföljande konsekvenser. Även om sekretess och konfidentialitet är en möjlig underliggande faktor, tyder mycket på att även ansvariga myndigheter har haft svårigheter att etablera en korrekt lägesbild. I Spanien bedömdes mörkertalet var stort i uppskattningar om vilka och hur många som drabbades av incidenterna.[299] I Indien var det enligt landets tidigare underrättelsechef svårt att kvantifiera utfallet av WannaCry, då många indiska organisationer inte ville medge att de utsatts. En kultur av bristande transparens bedömdes ha bidragit till svårigheter i att ta fram en pålitlig lägesbild.[300]

[295] Specker, Lawrence. "'Petya' cyberattack: Teamwork, pride fueled Alabama terminal's fight to rebound". *Advance Local*, 2017-07-09. https://www.al.com/news/index.ssf/2017/07/petya_cyberattack_teamwork_pri.html [Hämtad: 2019-03-28].

[296] Greenberg, Andy. "The untold story of NotPetya, the most devastating cyberattack in history". *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

[297] Kharkiv Airport. " Уважаемые пассажиры!". Facebook, 2017-06-27, [Översatt med Google Översätt]. https://www.facebook.com/hrk.aero/posts/1533337316697274:0 [Hämtad: 2019-04-01].

[298] *FactorDaily*, "Worldwide 'WannaCry' ransomware attack hit Andhra Police systems as well". 2017-05-13. https://factordaily.com/news/wannacry-ransomware-andhra-police/ [Hämtad: 2019-01-10].

[299] Palazuelos, Félix. " How the WannaCry ransomware attack affected businesses in Spain". *El País*, 2017-05-19. https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [Hämtad: 2019-02-06].

[300] *The Hindu*. 'WannaCry impact on India under-reported'. 2017-11-17. https://www.thehindu.com/news/cities/bangalore/wannacry-impact-on-india-under-reported/article20542868.ece [Hämtad: 2019-02-05].

I och med antagandet av NIS-direktivet finns det etablerade krav för leverantörer av samhällsviktig verksamhet att rapportera incidenter. [301] Baserat på rapportens material framstår det som om kryptomaskarna generellt inte orsakat störningar av den grad som krävs för att incidentrapporteringskraven ska inträda. Det återstår att se om incidentrapporteringen reglerad enligt NIS-direktivet kommer bidra med tidig varning om incidenter som potentiellt kan spridas och få tilltagande konsekvenser som blir betydande. I detta fall kan informella mekanismer och informationsdelning mellan leverantörer för samhällsviktig verksamhet och ansvariga myndigheter bli betydande.

4.3.2 Kommunikation, samverkan och transparens

Fallstudierna visar på variationer i kommunikation i samband med kryptomaskarna. I vissa länder sköttes kommunikationen på minister- eller departementsnivå, i andra länder var det kommunikationsansvariga på enskilda myndigheter eller i vissa fall företag som kommunicerade ut råd och information. I några fall skedde den främsta kommunikationen via den nationella CERT:en eller CSIRT:en. Informationssäkerhetschefer från det svenska näringslivet betonade exempelvis efter WannaCry-utbrottet att de lyckats undvika infektioner bland annat tack vare tidig information från CERT-SE.[302] Kommunikationen fokuserade främst på att tydliggöra vilka säkerhetsuppdateringar som drabbade och organisationer i riskzonen borde genomföra för att stoppa eller förhindra infektioner av WannaCry.

I exempelvis Indien involverades polis, som inledde brottsutredningar efter att incidenter rapporterats.[303] Även i Sverige är incidenter av den art som beskrivs i denna rapport kriminaliserade och NIS-direktivet har kontaktytor mot rättsvårdande myndigheter. Direktivet föreskriver samarbete och samråd i enlighet med nationell rätt mellan den myndighet som är utsedd till national kontaktpunkt för implementeringen av direktivet och relevanta rättsvårdande myndigheter och nationella dataskyddsmyndigheter.[304] I vissa fall, såsom vid brittiska NHS, kan det även vara lämpligt att incidenter efterföljs av en transparent utredning från tillsynsmyndigheter, särskilt då kryptomasken riskerade hanteringen av personuppgifter. Den typen av utredningar kan ha flera underliggande syften, exempelvis att identifiera svagheter i säkerhetsarbetet för att öka beredskap inför framtida incidenter, utkräva rättsligt ansvar och stärka allmänhetens tillit genom att signalera att säkerhet och ansvar är viktigt.

Informationsdelning under pågående incident har visat sig vara bristfällig, av varierande natur och ha många aktörer involverade. Det kan dessutom råda målbildskonflikter mellan snabb information och korrekt information. Därför är det viktigt att både incidentrapportering och kriskommunikation övas så att den är effektiv i skarpt läge.[305]

[301] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen EUT L 194, 19.7.2016, Artikel 14. https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[302] Rosengren, Lina. ”Svenska cio:er: så klarade vi oss från WannaCry”. *CIO Sweden*, 2017-06-05. https://cio.idg.se/2.1782/1.683866/svenska-cioer-wannacry [Hämtad: 2019-03-28].

[303] Press Trust of India, ”Ransomware Attack: Odisha’s govt hospital falls prey to WannaCry virus”. *LiveMint*, 2017-05-17.
https://www.livemint.com/Technology/X76bZbPH4nN4w7MaXN6tZL/Ransomware-attack-Odishas-govt-hospital-falls-prey-to-Wann.html [Hämtad: 2019-01-10].

[304] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen EUT L 194, 19.7.2016, Artikel 8.

[305] *NISÖ 2018. Erfarenhetsrapport*. Myndigheten för samhällsskydd och beredskap, 2018. ISBN 978-91-7383-900.

5 Slutsatser

Detta kapitel presenterar slutsatserna av rapportens fallstudie och analys, samt rekommendationer för framtida cybersäkerhetsarbete och forskning.

5.1 Kryptomaskarnas konsekvenser

WannaCry och NotPetya hade gemensamt att de båda var kryptomaskar, dvs. självspridande skadlig datorkod som krypterar innehåll i system för att neka användaren tillgång. WannaCry var därutöver ett fungerande gisslanprogram som krävde en lösensumma för att låsa upp systemet igen. WannaCrys funktion präglades därför av ekonomiska motiv, och spreds brett hos organisationer som hade låg cyberhygien. NotPetya såg på ytan ut som ett gisslanprogram, men anses vara en riktad attack mot ukrainska organisationer, troligtvis med rysk statlig sponsring. Spridningen var koncentrerad till Ukraina eftersom den skadliga koden distribuerades genom en bakdörr i den ukrainska redovisningsmjukvaran M.E.Doc, men koden spreds sig sedan från dotterbolag i Ukraina till andra länder genom organisationers interna nätverk.

Båda kryptomaskarna gav snabbt upphov till ett stort antal incidenter. Trots detta ter sig störningar i organisationers primära tjänstleveranser ha varit begränsade. Främst administrativa system verkar ha drabbats och ingen av de drabbade organisationerna rapporterade störningar i driften av, eller i system inuti, exempelvis flygplan, fartyg, tunnelbana eller tåg. Viss medicinteknisk utrustning samt containerterminalsystem var dock sårbara och infekterades. Organisationer som till hög grad var beroende av administrativa system för den primära tjänsteleveransen, så som i offentlig förvaltning, fick däremot störningar i tjänsteleveransen till följd av kryptomaskarna. Inga dödsfall eller allvarliga konsekvenser för allmän säkerhet till följd av störningarna har kunnat identifieras i materialet. De observerade konsekvenserna har främst varit ekonomiska. I de fall där organisationers verksamhetskontinuitet störddes blev de ekonomiska konsekvenserna större, eftersom kostnader för verksamhetsbortfall tillkom utöver kostnaderna för att återställa IT-system.

Vissa drabbade organisationer hade god förmåga att övergå till alternativa rutiner och klarade sig väl trots störningar i organisationens IT-system. Stora skillnader existerade dock mellan de drabbade organisationernas primära tjänsteleveranser samt vilka system som krävdes för leveransen. Dessa skillnader innebar även en varierande svårighet i att återskapa verksamhetskontinuitet. Trots att vissa organisationer drabbades av kryptomaskarna, undkom många organisationer både incidenter och störningar genom förebyggande åtgärder, god informationsdelning och kontinuitetshantering.

5.2 Att bemöta kryptomaskar

Det var främst nedprioriterat arbete med cyberhygien inom de drabbade organisationerna som gjorde dem sårbara för kryptomaskarna. Proaktiva åtgärder så som korrekt nätverkssegmentering, säkerhetskopiering, och uppdaterade system begränsade kryptomaskarnas spridning och konsekvenser. Rapporten kunde konstatera att Sverige låg bättre till gällande användning av licensierad mjukvara än länder som drabbades hårt av kryptomaskarna, vilket möjliggjorde installationen av säkerhetsuppdateringar som förhindrade infektion av WannaCry.

Som en del av arbetet med att höja organisationers cyberhygien rekommenderas att skapa riskanalyser av den typ lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster redan föreskriver, förbättra riskhantering och riskmedvetenhet, förankra och öva incidenthanteringsplaner, samt säkerställa installationen av säkerhetsuppdateringar.

Ett effektivt bemötande av kryptomaskar ställer krav på att incidentrapportering fångar upp incidenter tidigt, för att möjliggöra en bättre incidenthantering för både drabbade organisationer och myndigheter. God kommunikation och samverkan mellan ansvariga myndigheter och organisationer som riskerade drabbas ansågs ha varit en bidragande faktor till att svenska organisationer implementerat rätt förebyggande åtgärder, och sedermera klarade sig bättre undan WannaCry. Genom att tidigt identifiera ett utbrott av kryptomaskar kan det vara möjligt att begränsa spridningen genom att föreslå förebyggande åtgärder för de som ännu inte drabbats av det aktuella utbrottet. Effektiv informationsdelning möjliggör på så vis förebyggande åtgärder som är anpassade för det aktuella utbrottet av skadlig kod och kan även ge viss förvarning för incidenter. Därför ter sig en säkerhetskultur präglad av transparens och informationsdelning mellan drabbade organisationer och myndigheter, samt myndigheter sinsemellan, vara viktig.

Båda kryptomaskarna spreds snabbt på grund av att relativt lindriga förebyggande åtgärder inte vidtagits. Att NotPetya skickades ut genom en bakdörr till en välanvänd redovisningsmjukvara, samt hade en mer avancerad spridningsmekanism, gjorde den ännu svårare att förutse och förebygga. Avancerad spridningsförmåga hos skadlig kod ställer högre krav på organisationer att upprätthålla verksamhetskontinuitet när förebyggande åtgärder inte räcker till. Det går inte att utesluta att framtida hot likt NotPetya kan vara avancerade nog att förebyggande åtgärder inte räcker till för att skydda organisationer och myndigheter. Därför bör organisationer, baserat på sin riskanalys, bedriva kontinuitetsplanering för att begränsa inverkan på verksamhetskontinuiteten vid incidenter i IT-system.

Det är möjligt att organisationer med hög cyberhygien och god kontinuitetshantering kan begränsa konsekvenser i den egna organisationen men fortfarande agera infektionsvektor till andra organisationer. Därför behöver infektioner av kryptomaskar inte nödvändigtvis få stora konsekvenser för en organisation, men kan däremot spridas väldigt snabbt till andra organisationer där konsekvenserna kan bli allvarligare. Om rapporteringsplikten till ansvariga myndigheter enbart är baserad på incidenters allvar eller storlek kan spridningen av kryptomaskar bli större eftersom incidentrapporter inte inkommer tidigt.

Genom att kombinera god cyberhygien, förmåga att upprätthålla verksamhetskontinuitet och effektiv informationsdelning kan kryptomaskars spridning och konsekvenser begränsas, men sannolikt inte stoppas helt. Det går inte att utesluta att kryptomaskar i framtiden kan komma att antingen direkt drabba, eller orsaka kaskadeffekter som drabbar, leverantörer av samhällsviktiga tjänster. Övningen och utvärderingen av incidentrapporteringssystem kan därför med fördel undersöka om incidenter av skadlig kod med hög spridningsförmåga fångas upp innan de når gränsen för rapporteringsplikt till ansvariga myndigheter.

Rapportens material har begränsningar. Dels används material på få språk trots att kryptomaskarna fick internationell spridning, dels har nyhetsmediers rapportering inte alltid gått på djupet och gett en heltäckande bild av incidenterna och dess konsekvenser. Dessutom existerar fortfarande en kultur kring cybersäkerhet där organisationer gärna ger sken av att man gått oskadda ur en incident eller helt enkelt inte drabbats, eftersom om sådan information når media kan det innebära att allmänhetens förtroende för organisationen försämras eller att brottslig oaktsamhet uppdagas och leder till sanktioner. Det innebär att nyhetsrapportering kan återge en förskönad bild av incidenters inverkan på verksamheter. Vidare studier om kryptomaskar kan med fördel därför ta sig an ett djupare källmaterial, på fler språk, än denna rapport.

6 Litteraturförteckning

2017 Annual Report. A.P. Møller- Mærsk A/S, 2017. https://investor.maersk.com/static-files/5d68faa5-f869-4c08-8a1d-9660fe889360 [Hämtad: 2019-04-08].

AFP / The Local. “International cyber attacks put ransoms on German rail station screens”. *The Local*, 2017-05-13. https://www.thelocal.de/20170513/international-cyber-attacks-put-ransoms-on-german-train-departure-boards [Hämtad: 2019-03-27]

Alonso, Alejandro. “The Spanish Wholesale Gas Market”. National Energy Commission [Spanien], [Presentation], n.d. https://www.efet.org/Files/Documents/Press/Energy%20Trading%20Analyses/Third%20Party%20Publications//Presentacion%20CNE.pdf [Hämtad: 2019-02-06].

Al-Rimy, B.A.S., Maarof, M.A. och Shaid, S.Z.M. 2018. "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions", *Computers & Security* 74 (2018), s. 144-166.

Alvarez, Raul. ”Key Differences Between Petya and NotPetya”. *Fortinet*, 2017-07-09. https://www.fortinet.com/blog/threat-research/key-differences-between-petya-and-notpetya.html [Hämtad: 2019-03-27].

APM Terminals Mumbai. ”Welcome to APM Terminals Mumbai”. U.d. https://www.apmtmumbai.com/ [Hämtad: 2019-03-29].

Barrow, Keith. “German Monopoly Commission challenges DB dominance”. *International Railway Journal*, 2017-09-01. https://www.railjournal.com/in_depth/german-monopoly-commission-challenges-db-dominance [Hämtad: 2019-02-14].

Bazaraa, Danya. “These are the '74 countries hit by 45,000 WannaCry cyber attacks - and Russia is worst affected'”. *The Mirror*, 2017-05-15. https://www.mirror.co.uk/tech/74-countries-hit-45000-wannacry-10411971 [Hämtad: 2019-02-06].

BBC News. “Cyber-attack: US and UK blame North Korea for WannaCry”. 2017-12-19. https://www.bbc.com/news/world-us-canada-42407488 [Hämtad: 2019-03-27].

BBC News. “Ransomware cyber-attack: Who has been hardest hit?”. 2017-05-15. https://www.bbc.com/news/world-39919249 [Hämtad: 2019-02-06].

Bisson, David. ”NotPetya: Timeline of a Ransomworm”. *Tripwire The State of Security* [blogg], 2017-07-28. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/ [Hämtad: 2019-03-26].

Borys, Christian. “Ukraine braces for further cyber-attacks”. *BBC*, 2017-07-27. https://www.bbc.com/news/technology-40706093 [Hämtad: 2019-03-26].

Brewster, Thomas. “Another Massive Ransomware Outbreak Is Going Global Fast”. *Forbes*, 2017-06-27. https://www.forbes.com/sites/thomasbrewster/2017/06/27/ransomware-spreads-rapidly-hitting-power-companies-banks-airlines-metro/#62ae1fb27abd [Hämtad: 2019-03-27].

Brewster, Thomas. “NotPetya Ransomware Hackers ‘Took Down Ukraine Power Grid”. *Forbes*, 2017-07-03. https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/#c5e18886b89d [Hämtad: 2019-03-26].

Brito, Jerry och Watkins, Tate. “Loving the cyber bomb-the dangers of threat inflation in cybersecurity policy”. *Harvard National Security Journal* 3, nr. 1 (2018): 39-84.

Burnson, Patrick. “Port of Los Angeles reacts to Petya Crisis as CargoSmart Provides Some Supply Chain Solutions”. *Supply Chain Management Review*, 2017-06-28. http://www.scmr.com/article/port_of_los_angeles_reacts_to_pety_crisis_as_cargosmart_provides_some_suppl [Hämtad: 2019-03-27].

Cadell, Cate; Jourdan, Adam och Gopalakrishnan, Raju. “Cyber attack hits China government, schools, but spread slows”. *Reuters*, 2017-05-15. https://www.reuters.com/article/us-cyber-attack-china-idUSKCN18B10H [Hämtad: 2019-02-05]

Carrie Wong, Julia och Solon, Olivia. ”Massive ransomware cyber-attack hits nearly 100 countries around the world”. *The Guardian*, 2017-05-12. https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs [Hämtad: 2019-02-06].

CBS Los Angeles. ”Global Cyberattack Shuts Down Port of LA’s Largest Terminal. https://losangeles.cbslocal.com/2017/06/27/cyberattack-port-of-la/

CCN-CERT. “Identificado ataque de ransomware que afecta a sistemas Windows“. 2017-05-12. https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html [Hämtad: 2019-02-06].

Censor.net. ”List of Ukrainian companies and agencies whose websites were attacked by hackers on June 27 (live updates)”. 2017-06-27. https://en.censor.net.ua/n445650 [Hämtad: 2019-02-15]; GroupIB. ”Petya starts with Ukraine and then goes global”. 2017-06-27. https://www.group-ib.com/blog/petya. [Hämtad: 2019-03-27].

CERT-EU. ”CERT-EU Security Advisory 2017-014 Petya-Like Malware Campaign“. 2017-06-29. https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-014.pdf [Hämtad: 2019-02-18].

CERT-IN. ”Advisory CIAD-2017-0024. Wannacry/ WannaCrypt Ransomware – CRITICAL ALERT”. 2017-05-14. Tillgänglig på https://www.cert-in.org.in/. [Hämtad: 2019-03-27].

CERT-SE. ”Nytt angrepp av utpressningsprogram”. 2017-06-27. [Arkiverad] https://web.archive.org/web/20170627171605/https://www.cert.se/2017/06/nytt-angrepp-av-utpressningsprogram [Hämtad: 2019-02-18].

CERT-SE. ”Om CERT-SE”. 2019-01-22. https://www.cert.se/om-cert-se [Hämtad: 2019-03-27].

Cherepanov, Anton. “Analysis of Telebots’s cunning backdoor”. ESET, 2017-07-04. https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ [Hämtad: 2019-02-15].

Cherepanov, Anton. ”TeleBots are back: Supply-chain attacks against Ukraine. *We Live Security*, 2017-06-30. https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/ [Hämtad: 2019-03-27].

Chirgwin, Richard. “IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz”. *The Register*, 2018-01-25. https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/ [Hämtad: 2019-02-15].

Chornokondratenko, Margaryta. “Ukraine power company says was hit by second cyber attack”. *Reuters*, 2017-06-30. https://www.reuters.com/article/uk-cyber-attack-ukrenergo/ukraine-power-company-says-was-hit-by-second-cyber-attack-idUKKBN19L0OM [Hämtad: 2019-02-15].

Cimpanu, Catalin. “New Data Shows Most WannaCry Victims Are From China, Not Russia”. *Bleeping Computer*. https://www.bleepingcomputer.com/news/security/new-data-shows-most-wannacry-victims-are-from-china-not-russia/ [Hämtad: 2019-02-05].

COM 2017/476: MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET: Maximalt utnyttjande av it-säkerhetsdirektivet – mot ett effektivt genomförande av direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks och informationssystem i hela unionen. Bilaga.

Cristales, Denny. ”Homeland Security Committee examined LA Ports’ cyber protection and vulnerabilities at field hearing”. *Signal Tribune*, 2017-11-03. https://signaltribunenewspaper.com/35673/news/homeland-security-committee-examined-la-ports-cyber-protection-and-vulnerabilities-at-field-hearing/ [Hämtad: 2019-03-29].

Crosby, Alan. “Ukraine Is ‘Ground Zero’ For Hackers In Global Cyberattacks”. *Radio Free Europe Radio Liberty*, 2017-06-28. https://www.rferl.org/a/ukraine-petya-ransomware-cyberattack-ground-zero/28583931.html [Hämtad: 2019-03-26]; Polityuk, Pavel. ”Ukraine points finger at Russian security services in recent cyber attack”. *Reuters*, 2017-07-01. https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P [Hämtad: 2019-03-26].

Curtis, Sophie. “Chernobyl nuclear power plant hit by 'Petya' ransomware attack causing havoc across the globe”. *Daily Mirror*, 2017-06-27. https://www.mirror.co.uk/tech/chernobyl-nuclear-power-plant-hit-10697960 [Hämtad: 2019-02-15].

D’Souza-Wiltshire, Iaan; Schonning, Nick; Mackenzie, Duncan; Hall, Justin. “WannaCrypt Ransomware worm targets out-of-date systems”. Windows IT Pro Center, 2017-07-27. https://docs.microsoft.com/en-us/windows/security/threat-protection/wannacrypt-ransomware-worm-targets-out-of-date-systems-wdsi [Hämtad: 2019-03-27].

DailyHunt, ”Ransomware attack: Govt hospitals continue to fall prey”, 2017-05-20. https://m.dailyhunt.in/news/india/english/odishatv-epaper-odishatv/ransomware+attack+govt+hospitals+continue+to+fall+prey-newsid-67878733 [Hämtad: 2019-01-10].

Das, Lalit. ”The advisory for Ransomware Threat-’WannaCry’”. Government of Odisha Home Department. http://www.homeodisha.gov.in/sites/default/files/AddFiles/WANNACRY.pdf [Hämtad: 2019-03-27].

Davis, Jessica. ”West Virigina hospital replaces computers after Petya cyberattack”. *Healthcare IT News*, 2017-06-30. https://www.healthcareitnews.com/news/west-virginia-hospital-replaces-computers-after-petya-cyberattack [Hämtad: 2019-03-29].

de Haldevang, Max och Collins, Keith. ”The cyber attack that knocked out Ukraine this morning is now going global”. *Quartz.com*, 2017-06-27. https://qz.com/1015755/ukraine-cyber-attack-the-petyapetrwrap-ransomware-with-similarities-to-wannacry-is-now-going-global/ [Hämtad: 2019-02-15].

Dearden, Lizzie. “Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers“.*The Independent,* 2017-06-27. https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html [Hämtad: 2019-02-15]

DNA India, ”Odisha: City hospital system down, officials fear 'WannaCry' attack”. 2017-05-17. https://www.dnaindia.com/india/report-odisha-city-hospital-system-down-officials-fear-wannacry-attack-2441803 [Häntdatum: 2019-02-05].

Duckett, Chris. “Ransomware in disguise: Experts say Petya out to destroy not ransom”. *ZDNet*, 2917-06-29. https://www.zdnet.com/article/ransomware-in-disguise-experts-say-petya-out-to-destroy-not-ransom/ [Hämtad: 2019-03-27].

ENISA, 2016. ”Review of Cyber Hygiene practices”. DOI 10.2824/352617. https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport [Hämtad: 2019-03-27]

ENISA. ”WannaCry Ransomware Outburst”. 2017-05-15. https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst [Hämtad: 2019-03-27].

ET Bureau. “India third worst hit nation by ransomware Wannacry; over 40,000 computers affected”. *The Economic Times*, 2017-05-17. https://economictimes.indiatimes.com/tech/internet/india-third-worst-hit-nation-by-ransomware-wannacry-over-40000-computers-affected/articleshow/58707260.cms [Hämtad: 2019-02-05].

Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen EUT L 194, 19.7.2016, s. 1–30.

FactorDaily, ”Worldwide ’WannaCry’ ransomware attack hit Andhra Police systems as well”. 2017-05-13. https://factordaily.com/news/wannacry-ransomware-andhra-police/ [Hämtad: 2019-01-10].

FedEx. “FedEx Files 10-K with Additional Disclosure on Cyber-Attack Affecting TNT Express Systems”. 2017-07-17. http://investors.fedex.com/news-and-events/investor-news/news-release-details/2017/FedEx-Files-10-K-with-Additional-Disclosure-on-Cyber-Attack-Affecting-TNT-Express-Systems/default.aspx [Hämtad: 2019-03-29].

Fruhlinger, Josh. ”Petya ransomware and NotPetya malware: What you need to know now”. *CSO Online*, 2017-10-17. https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html [Hämtad: 2019-03-27].

Fruhlinger, Josh. ”The 5 biggest ransomware attacks of the last 5 years”. *CSO Online*, 2017-08-01. https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html [Hämtad: 2019-03-27].

Fulbright, Norton Rose. “WannaCry Ransomware Attack Summary”. *Data Protection Report*, 2017-05-17. https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/ [Hämtad: 2019-03-27].

Glaser, April. ”U.S hospitals have been hit by the global ransomware attack”. *Recode*, 2017-06-27. https://www.recode.net/2017/6/27/15881666/global-eu-cyber-attack-us-hackers-nsa-hospitals [Hämtad: 2019-03-27].

Goncharova, Olena; Grytsenko, Oksana och Krasnikov, Denys. ”Ukraine finds itself at the epicenter of global cyberattack. *Kyiv Post*, 2017-06-30. https://www.pressreader.com/ukraine/kyiv-post/20170630/281741269437161 [Hämtad: 2019-02-15].

Goodin, Dan. “An NSA-derived ransomware worm is shutting down computers worldwide”. *Ars Technica*, 2017-05-12. https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/ [Hämtad: 2019-02-06].

Greenberg, Andy. “The untold story of NotPetya, the most devastating cyberattack in history”. *Wired*, 2018-08-22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2019-02-15].

Heller, Michael. ”Lazarus Group hacker charged in WannaCry, Sony atacks”. SearchSecurity, 2018-11-07. https://searchsecurity.techtarget.com/news/252448325/Lazarus-Group-hacker-charged-in-Wannacry-Sony-attacks [Hämtad: 2019-03-27].

Hern, Alex. “Ransomware attack 'not designed to make money', researchers claim”. *The Guardian*, 2017-06-28. https://www.theguardian.com/technology/2017/jun/28/notpetya-ransomware-attack-ukraine-russia [Hämtad: 2019-02-15].

Hern, Alex. “WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017”. *The Guardian*, 2017- 12-30. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware [Hämtad: 2019-03-27].

Hersey, Frank. “Here’s what we know about how WannaCry has affected China”. *TechNode*, 2017-05-15. https://technode.com/2017/05/15/how-hard-did-wannacry-virus-hit-china/ [Hämtad: 2019-02-05]

Hindustan Times. ”WannaCry ransomware: Andhra police fall prey to global cyber attack”, 2017-05-16. https://www.hindustantimes.com/india-news/wannacry-ransomware-andhra-police-fall-prey-to-global-cyber-attack/story-FkQZQHepiIAlVMJTobKLfN.html [Hämtad]

Hindustan Times. ”’WannaCry’ ransomware: Bengal power distribution company hit by cyberattack, say officials, say officials”, 2017-05-15. https://www.hindustantimes.com/india-news/wannacry-ransomware-bengal-power-distribution-company-hit-by-cyberattack-say-officials/story-biqMQN5cPKng36cIyho2oJ.html [Hämtad: 2019-01-10].

Hughes, Owen. “WannaCry one year on: a retrospective look at NHS IT’s black-letter day”. *DigitalHealth.net*, 2018-05-11. https://www.digitalhealth.net/2018/05/wannacry-one-year-on/ [Hämtad: 2019-02-14].

IANS. “Andhra Pradesh’s police departments affected by ‘WannaCry’ ransomware”. *BGR*, 2017-05-16. https://www.bgr.in/news/andhra-pradeshs-police-departments-affected-by-wannacry-ransomware/ [Hämtad: 2019-03-29].

IANS. ”Indian government has started taking measures to protect itself from the latest ransomware attack”. *First Post*, 2017-06-28. https://www.firstpost.com/tech/news-analysis/indian-government-has-started-taking-measures-to-protect-itself-from-the-latest-ransomware-attack-3835135.html [Hämtad: 2019-02-18].

Indian Express. “WannaCry ransomware: Computers at West Bengal State electricity firm hit”. 2017-05-15. https://indianexpress.com/article/technology/tech-news-technology/wannacry-ransomware-computers-at-west-bengal-state-electricity-firm-hit/ [Hämtad: 2019-02-05].

Interfax-Ukraine. ”Kyivenergo hacked, Ukrenergo affected”. *Kyiv Post*, 2017-06-27. https://www.kyivpost.com/ukraine-politics/kyivenergo-hacked-ukrenergo-affected.html [Hämtad: 2019-02-15].

Investigation: WannaCry cyber attack and the NHS. London: National Audit Office, 2017. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Hämtad: 2019-02-14].

Israelsson, Fredrik. ”Personal på hemtjänsten fick ta fram papper och penna”. *SVT*, 2017-05-15. https://www.svt.se/nyheter/lokalt/vasternorrland/personalen-fick-ta-fram-papper-och-penna [Hämtad: 2019-02-14].

Ivanonov, Anton och Mamedov, Orkhan. ”ExPetr/Petya/NotPetya is a Wiper, Nor Ransomware”. *SecureList*, 2017-06-28. https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ [Hämtad: 2019-03-26]

Jawaharlal Nehru Port. “The Birth of JNPT”. 2018-09-28. http://jnport.gov.in/ [Hämtad: 2019-03-29].

Kaste, Martin. ”From Kill Switch To Bitcoin, ’WannaCry’ Showing Signs Of Amateur Flaws”. *National Public Radio* [webbsida], 2017-05-16. https://www.npr.org/sections/alltechconsidered/2017/05/16/528570788/from-kill-switch-to-bitcoin-wannacry-showing-signs-of-amateur-flaws?t=1537969494161 [Hämtad: 2019-03-27].

Kharkiv Airport. ”Уважаемые пассажиры!”. Facebook, 2017-06-27, [Översatt med Google Översätt]. https://www.facebook.com/hrk.aero/posts/1533337316697274:0 [Hämtad: 2019-04-01].

Kohmami, Nadia & Solon, Olivia. ”’Accidental hero’ halts ransomware attack and warns: this is not over”. *The Guardian*, 2017-05-13. https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack [Hämtad: 2019-03-27].

Kottasová, Ivana. ”Why Russia's cyber defenses are so weak”. *CNN*, 2015-05-15. https://money.cnn.com/2017/05/15/technology/russia-vulnerable-cyberattack/index.html [Hämtad: 2019-02-06].

Kryptos Logic. ”WannaCry: Two Weeks and 16 Million Averted Ransoms Later”. 2017-05-29. https://blog.kryptoslogic.com/malware/2017/05/29/two-weeks-later.html [Hämtad: 2019-03-27].

Kubovič, Ondrej. ”Ransomware is everywhere, but even black hats make mistakes”. *We Live Security* [del av ESET], 2016-04-28. https://www.welivesecurity.com/2016/04/28/ransomware-is-everywhere-but-even-black-hats-make-mistakes/ [Hämtad: 2019-03-27].

Lam, Oiwan. ”Why is China Home to Half of the Computers Infected With WannaCry Ransomware?”, *GlobalVoices Advox*, 2017-05-16. https://advox.globalvoices.org/2017/05/16/why-is-china-home-to-half-of-the-computers-infected-with-wannacry-ransomware/ [Hämtad: 2019-02-05]

Lewis, James Andrew. *Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage*. Washington: Center for Strategic & International Studies, 2014. http://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140313_FireEye_WhitePaper_Final.pdf [Hämtad: 2019-03-27].

Lindblom, Hans. ”Timrå kommun hade gammalt virusskydd”. *SVT*, 2017-10-29. https://www.svt.se/nyheter/lokalt/vasternorrland/timra-kommun-hade-gammalt-virusskydd [Hämtad: 2019-02-14].

LiveMint. ”Ransomware Attack: Odisha’s govt hospital falls prey to WannaCry virus”, 2017-05-17. https://www.livemint.com/Technology/X76bZbPH4nN4w7MaXN6tZL/Ransomware-attack-Odishas-govt-hospital-falls-prey-to-Wann.html [Hämtad: 2019-01-10].

Maynor, David; Nikolic, Aleksandar; Olney, Matt och Younan, Yves. ”The M.E.Doc Connection”. *Talo Intelligence*, 2017-07-05. https://blog.talosintelligence.com/2017/07/the-M.E.Doc-connection.html [Hämtad: 2019-03-26].

McNeil, Adam. “How did the WannaCry ransomworm spread?”. *Malwarebytes Labs*, 2017-05-19. https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/ [Hämtad: 2019-03-27].

Microsoft MSRC Team. “Customer Guidance for WannaCrypt attacks”. *Microsoft TechNet*, 2017-05-12. https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ [Hämtad: 2019-03-27].

Moore-Colyer, Roland. “WannaCry Wallops Russian Post, Highlightning The Risk Of Legacy IT”. *Silicon*, 2017-05-25. https://www.silicon.co.uk/security/wannacry-russian-post-213099 [Hämtad: 2019-03-27].

MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. https://www.msb.se/externdata/rs/9b5c0905-20c5-4fe6-8341-5b481cc570a4.pdf [Hämtad: 2019-03-26].

MSBFS 2018:9 Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster. https://www.msb.se/Upload/Om%20MSB/Lag_och_ratt/F%C3%B6rfattningar/MSBFS2018_9.pdf [Hämtad: 2019-03-26].

Myndigheten för samhällsskydd och beredskap. ”FAQ om WannaCry”. 2017-05-15. https://www.msb.se/sv/Insats--beredskap/Pagaende-handelser-och-insatser/Tidigare-handelser/IT-attacken-WannaCryransomware/FAQ-om-WannaCry/ [Hämtad: 2019-02-06].

Nakashima, Ellen. ”Russian military was behind ‘NotPetya’ attack in Ukraine, CIA concludes”. *Washington Post*, 2018-01-02. https://www.washingtonpost.com/world/national-

security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html [Hämtad: 2019-03-26].

Nasr, Joseph och Heinrich, Mark. ”German rail operator affected by global cyber attack”. *Reuters*, 2017-05-13. https://www.reuters.com/article/us-cyber-attack-germany-rail-idUSKBN1890DM [Hämtad: 2019-02-14].

National Bank of Ukraine. “The National Bank of Ukraine Warned Banks and other Financial Market Participants about an External Hacker Attack”. 2017-06-27. https://bank.gov.ua/control/en/publish/article?art_id=51024813 [Hämtad: 2019-02-15].

NDTV, “More Computers In Bengal’s Electricity Distribution Offices Attacked By ’Wannacry”, 2017-05-16. https://www.ndtv.com/india-news/more-computers-in-west-bengal-state-electricity-distribution-companys-offices-attacked-by-wannacry-1694383 [Hämtad: 2019-01-10].

Nekham, Erika. ”Ingen "måndagsvåg" av virusattacken”. *Norbottens Kuriren*, 2017-05-15. https://www.kuriren.nu/nyheter/ingen-mandagsvag-av-virusattacken-nm4545730.aspx [Hämtad: 2019-02-14].

Newman, Lily Hay. ”How an accidental ‘kill switch’ slowed Friday’s massive ransomware attack”. *Wired*, 2017-05-13. https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/ [Hämtad: 2019-03-27].

NISÖ 2018. Erfarenhetsrapport. Myndigheten för samhällsskydd och beredskap, 2018. ISBN 978-91-7383-900.

Nyberg, Katinka. ”Var uppmärksammad på Ransomware”. Atrox, u.d. https://atrox.se/var-uppmarksammad-pa-ransomware/ [Hämtad: 2019-03-27].

O’Connor, Fred. ”NotPetya still roils company´s finances costing organizations $1.2 billion in revenue”. Cyberreason, 2017-11-09. https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue [Hämtad: 2019-03-27].

Odisha Sun Times, “Odisha govt issues advisory on WannaCry Ransomware”. 2017-05-17. https://odishasuntimes.com/odisha-govt-issues-advisory-on-wannacry-ransomware/ [Hämtad: 2019-02-05].

Offshore Energy Today. “Maersk, Rosneft hit by cyberattack”. 2017-06-28. https://www.offshoreenergytoday.com/report-maersk-rosneft-hit-by-cyberattack/ [Hämtad: 2019-02-18].

Palazuelos, Félix. ” How the WannaCry ransomware attack affected businesses in Spain”. *El País*, 2017-05-19. https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [Hämtad: 2019-02-06].

“PARK JIN HYOK”. FBI. 2018-08-30. https://www.fbi.gov/wanted/cyber/park-jin-hyok [Hämtad: 2019-03-27].

Perlroth, Nicole; Scott, Mark och Frenkel, Sheera. “Cyberattack Hits Ukraine Then Spreads Internationally”. *New York Times*, 2017-06-27. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html [Hämtad: 2019-03-27].

Piper, Elizabeth och Heinrich, Mark. “Cyber attack hits 200,000 in at least 150 countries: Europol. *Reuters*, 2017-05-14. https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX [Hämtad: 2019-03-27].

Polityuk, Pavel och Auchard, Erik. “Global cyber attack likely cover for malware installation in Ukraine: police official“. *Reuters*, 2017-06-29. https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19K1WI [Hämtad: 2019-02-15].

Polityuk, Pavel. ”Ukraine points finger at Russian security services in recent cyber attack”. *Reuters*, 2017-07-01. https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P [Hämtad: 2019-03-26].

Polityuk, Pavel; Prentice, Alessandra och Pomeroy, Robin. “Kiev airport hit by cyber attack, delays possible”. *Reuters*, 2017-06-27. https://www.reuters.com/article/us-cyber-attack-ukraine-airport/kiev-airport-hit-by-cyber-attack-delays-possible-idUSKBN19I1OR?il=0 [Hämtad: 2019-02-15].

Port of Rotterdam Authority. ”Facts and figures”. U.d. Tillgänglig via https://www.portofrotterdam.com/sites/default/files/facts-and-figures-port-of-rotterdam.pdf?token=CJ3nvKBO [Hämtad: 2019-03-29].

Port of Rotterdam. “More vessels call on a safe port”. 2018-01-15. https://www.portofrotterdam.com/en/news-and-press-releases/more-vessels-call-on-a-safe-port [Hämtad: 2019-02-18].

Press Trust of India, “Government Activates Response Mechanism To Prevent Cyber Attack”. *NDTV*, 2017-05-14. https://www.ndtv.com/india-news/government-activates-response-mechanism-to-prevent-cyber-attack-1693438 [Hämtad: 2019-02-05].

Press Trust of India, ”Ransomware Attack: Odisha’s govt hospital falls prey to WannaCry virus”. *LiveMint*, 2017-05-17. https://www.livemint.com/Technology/X76bZbPH4nN4w7MaXN6tZL/Ransomware-attack-Odishas-govt-hospital-falls-prey-to-Wann.html [Hämtad: 2019-01-10].

Reuters. ”China's banking regulator to step up protection after cyber attack”. 2017-05-17. https://www.reuters.com/article/us-cyber-attack-china-regulator/chinas-banking-regulator-to-step-up-protection-after-cyber-attack-idUSKCN18D0WZ [Hämtad: 2019-02-05]

Reuters. ”Cyber-attack: US and UK blame North Korea for WannaCry. 2017-12-19. https://www.bbc.com/news/world-us-canada-42407488 [Hämtad: 2019-03-27].

Rice, Adam. “Why WannaCry and other computer worms may inherit the earth”. *SearchSecurity*, 2017-09-01. https://searchsecurity.techtarget.com/feature/Why-WannaCry-and-other-computer-worms-may-inherit-the-earth [Hämtad: 2019-03-27].

Richter, Wolf. “China's use of pirated software left it vulnerable to the WannaCry ransomware attack”. *Business Insider*, 2017-05-16. https://www.businessinsider.com/wannacry-ransomware-attack-china-2017-5?r=US&IR=T&IR=T [Hämtad: 2019-02-05]

Rosengren, Lina. ”Svenska cio:er: så klarade vi oss från Wannacry”. *IDG.se*, 2017-06-05. https://cio.idg.se/2.1782/1.683866/svenska-cioer-wannacry [Hämtad: 2019-02-14].

RT. ” Russian banks, railway giant among targets of WannaCry ransomware allegedly linked to NSA”. 2017-05-13. https://www.rt.com/news/388228-wannacry-russian-railways-banks/ [Hämtad: 2019-02-05].

Ruano, Carlos; Rodriguez, Jose; Finkle, Jim; White, Sarah; Berwick, Angus och Lawrence, Jane. “Telefonica, other Spanish firms hit in "ransomware" attack”. *Reuters*, 2017-05-12. https://www.reuters.com/article/us-spain-cyber/telefonica-other-spanish-firms-hit-in-ransomware-attack-idUSKBN1881TJ [Hämtad: 2019-02-06].

Samlad informations och cybersäkerhetshandlingsplan för åren 2019–2022. Myndigheten för samhällsskydd och beredskap, 2019-03-01. ISBN 978-91-7383-918-1, https://www.msb.se/RibData/Filer/pdf/28804.pdf [Hämdatum: 2019-03-26].

Samson, Adam; McGee, Patrick; Hornby, Lucy; Zhang, Archie; Fildes, Nic och Inagaki, Kana. “WannaCry cyber attack highlights dilemma in fight against malware”. *Financial Times*, 2017-05-15. https://www.ft.com/content/bf29e8e0-3985-11e7-821a-6027b8a20f23 [Hämtad: 2019-02-14].

Satter, Raphael. ”Official: firm at center of cyberattack knew of problems”. *Associated Press.* https://apnews.com/8b02768224de485eb4e7b33ae55b02f2 [Hämtad: 2019-02-15].

Shalal, Andrea. “Germany's BSI says more German companies affected by cyber attacks”. *Reuters*, 2017-05-15. https://www.reuters.com/article/us-cyber-attack-germany/germanys-bsi-says-more-german-companies-affected-by-cyber-attacks-idUSKCN18B242 [Hämtad: 2019-02-14].

Shepherd, Adam. “NotPetya was nastier than WannaCry ransomware, say experts”. *IT Pro*, 2017-11-01. http://www.itpro.co.uk/security/29863/notpetya-was-nastier-than-wannacry-ransomware-say-experts [Hämtad: 2019-03-27].

Smart Energy International. “Iberdrola Producing more MWs in Mexico than Spain for 2018”. 2018-07-31. https://www.power-eng.com/articles/2018/07/iberdrola-producing-more-mws-in-mexico-than-spain-for-2018.html [Hämtad: 2019-04-01].

Smart, William. *Lessons learned review of the WannaCry Ransomware Cyber Attack*. London: National Health Service, 2018. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf [Hämtad: 2019-02-14].

Software Management: Security Imperative, Business Opportunity. The Software Alliance, 2018. https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf [Hämtad: 2019-04-01].

Specker, Lawrence. ”’Petya’ cyberattack: Teamwork, pride fueled Alabama terminal’s fight to rebound”. *Advance Local*, 2017-07-09. https://www.al.com/news/index.ssf/2017/07/petya_cyberattack_teamwork_pri.html [Hämtad: 2019-03-28].

“Statement from the Press Secretary”. White House, 2018-02-15. https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ [Hämtad: 2019-03-26].

Storm, Darlene. ”Cryptoworms: The future of ransomware hell”. *ComputerWorld*, 2016-04-13. https://www.computerworld.com/article/3055488/security/cryptoworms-the-future-of-ransomware-hell.html [Hämtad: 2019-03-27].

Stubbs, Jack. “Exclusive: Wannacry hits Russian postal service, exposes wider security shortcomings”. *Reuters*, 2017-05-24. https://uk.reuters.com/article/us-cyber-attack-russia/exclusive-wannacry-hits-russian-postal-service-exposes-wider-security-shortcomings-idUKKBN18K26O [Hämtad: 2019-02-06]

Stubbs, Jack. “Russia still reeling from WannaCry ransomware attack”. *Business Live*, 2017-05-25. https://www.businesslive.co.za/bd/world/europe/2017-05-25-russia-still-reeling-from-wannacry-ransomware-attack/ [Hämtad: 2019-02-05].

Stubbs, Jack. “Russian postal service brought down by WannaCry ransomware virus”. *The Independent*, 2017-05-25. https://www.independent.co.uk/life-style/gadgets-and-tech/news/russia-postal-service-wannacry-ransomware-cyber-virus-attack-windows-xp-a7754841.html [Hämtad: 2019-02-06].

Suiche, Matt. ”Petya.2017 is a wiper not a ransomware”. *Comae Technologies* [blogg], 2017-06-28. https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b. [Hämtad: 2019-04-08].

Sulleyman, Aatif. ”‘Petya' cyber attack: list of affected companies shows scale of hack“. *The Independent*, 2017-06-27. https://www.independent.co.uk/life-style/gadgets-and-tech/news/petya-cyber-attack-affected-companies-hack-wpp-rosneft-mondelez-deutsche-post-security-problems-a7811056.html [Hämtad: 2019-02-18].

Svensson, Anton och Quayle, Anna. ”Kommuner hårt drabbade av utpressningsvirus”. *SVT*, 2017-10-31. https://www.svt.se/nyheter/lokalt/vasternorrland/kommuner-hart-drabbade-av-utpressningsvirus [Hämtad: 2019-02-06].

Tenitskaja, Alexandra Carlsson och Dickson, Staffan. ”Storföretag drabbade av nätattack”. *Aftonbladet*, 2017-06-27. https://www.aftonbladet.se/nyheter/a/Ja618/hackerattack-mot-goteborgs-hamn [Hämtad: 2019-02-18].

The Hindu. ‘WannaCry impact on India under-reported’. 2017-11-17. https://www.thehindu.com/news/cities/bangalore/wannacry-impact-on-india-under-reported/article20542868.ece [Hämtad: 2019-02-05].

The Maritime Executive. “Maersk's Cargo Operations Hit Hard by Cyberattack”. https://www.maritime-executive.com/article/maersks-cargo-operations-hit-hard-by-cyberattack#gs.iTipKYI [Hämtad: 2019-02-15].

The State of IT Security in Germany 2017. Bonn: Federal Office for Information Security (BSI), 2017. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2017.pdf?__blob=publicationFile&v=3 [Hämtad: 2019-02-14]

"The WannaCry ransomware attack". *Strategic Comments* 23, nr. 4, 2017, s. vii-ix.

Thomson, Iain. “Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide”. *The Register*, 2017-06-28. https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/ [Hämtad: 2019-03-26].

Thomson, Iain. “Virus (cough, cough, Petya) goes postal at FedEx, shares halted”. *The Register*, 2018-06-28. https://www.theregister.co.uk/2017/06/28/fedex_tnt_express_virus_attack/ [Hämtad: 2019-02-18].

Toledano, Bruno. ” Hackean la red interna de Telefónica y de otras grandes empresas españolas”. *El Mundo*, 2017-05-12. https://www.elmundo.es/tecnologia/2017/05/12/59158a8ce5fdea194f8b4616.html [Hämtad: 2019-02-06].

Trevors, Matthew. ”Cyber Hygiene: 11 Essential Practices”. *Insider Threat Blog*, Carnegie Mellon University, 2017-11-15. https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html [Hämtad: 2019-03-27].

TT / NyTeknik. ”Göteborgs hamn svårt drabbad av it-attack”. *Ny Teknik*, 2017-06-28. https://www.nyteknik.se/digitalisering/goteborgs-hamn-svart-drabbad-av-it-attack-6858639 [Hämtad: 2019-02-18].

TT. ”Göteborgs hamn lamslagen av IT-attacken”. *Svenska Dagbladet*, 2017-06-28. https://www.svd.se/oklart-hur-virusattack-drabbar-sverige [Hämtad: 2019-02-18].

TT. ”Ingen akut ökning av virusdrabbade”. *Ny Teknik*, 2017-05-15. https://www.nyteknik.se/digitalisering/ingen-akut-okning-av-virusdrabbade-6848426 [Hämtad: 2019-02-14].

Ukrinform. ”Cyber attack on Ukrainian government and corporate networks halted”. 2017-06-28. https://www.ukrinform.net/rubric-polytics/2255698-cyber-attack-on-ukrainian-government-and-corporate-networks-halted.html [Hämtad: 2019-02-15].

Ukrinform. ”Stoltenberg: NATO to increase aid to Ukraine in field of cyber defense”. 2017-06-28. https://www.ukrinform.net/rubric-defense/2255739-stoltenberg-nato-to-increase-aid-to-ukraine-in-field-of-cyber-defense.html [Hämtad: 2019-03-26].

Urra, Susanna. ”How the WannaCry ransomware attack affected businesses in Spain”. *El País*, 2017-05-19. https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html [Hämtad: 2019-02-06].

Van Gompel, Marieke. ”WannaCry virus was ‘wake-up call’ for railway industry”. *RailTech.com*, 2017-12-11. https://www.railtech.com/all/2017/12/11/wannacry-virus-was-wake-up-call-for-railway-industry/ [Hämtad: 2019-02-14].

Wakefield, Jane. “Tax software blamed for cyber-attack spread”. *BBC*, 2017-06-28. https://www.bbc.com/news/technology-40428967 [Hämtad: 2019-02-15].

Warren, Tom. ”Microsoft issues ’highly unusual’ Windows XP patch to prevent massive ransomware attack”. *The Verge*, 2017-05-13. https://www.theverge.com/2017/5/13/15635006/microsoft-windows-xp-security-patch-wannacry-ransomware-attack [Hämtad: 2019-03-27].

Wattles, Jackie och Disis, Jill. “Ransomware attack: Who's been hit been hit”. *CNN*, 2017-05-15. https://money.cnn.com/2017/05/15/technology/ransomware-whos-been-hit/index.html [Hämtad: 2019-02-05].

We Live Security. “New WannaCryptor-like ransomware attack hits globally: All you need to know”. 2017-06-27. https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/ [Hämtad: 2019-03-27].

Wiklund, Kalle. ”Polisen: Så många svenskar har anmält Wannacry-utpressarna”. *Ny Teknik*, 2017-05-17. https://www.nyteknik.se/digitalisering/polisen-sa-manga-svenskar-har-anmalt-wannacry-utpressarna-6849119 [Hämtad: 2019-02-14].

Wiklund, Kalle. ”Timrå kommun: Miss hos it-leverantör öppnade för Wannacry”. *Ny Teknik*, 2017-05-17. https://www.nyteknik.se/digitalisering/timra-kommun-miss-hos-it-leverantor-oppnade-for-wannacry-6849137 [Hämtad: 2019-02-06].

Winning, Alexander och Stubbs, Jack. ”WannaCry cyber attack compromised some Russian banks: central bank”. *Reuters*, 2017-05-19. https://www.reuters.com/article/us-cyber-attack-russia-cenbank-idUSKCN18F16V [Hämtad: 2019-02-05].

Wisterberg, Erik. ”Hackare lamslår svenska företag – håller datorerna som gisslan”. *BreakIt*, 2017-06-27. https://www.breakit.se/artikel/8101/hackare-lamslar-svenska-foretag-haller-datorerna-som-gisslan [Hämtad: 2019-02-18].

Woollaston, Victoria. “Wanna Decryptor ransomware appears to be spawning and this time it may not have a kill switch”. *Wired*, 2017-05-16. https://www.wired.co.uk/article/wanna-decryptor-ransomware [Hämtad: 2019-03-27].

Yegorov, Oleg. “WannaCry hack: Why has Russia suffered more than other countries?”. *Russia Beyond*, 2017-05-16. https://www.rbth.com/international/2017/05/16/wannacry-hack-why-has-russia-suffered-more-than-other-countries_763869 [Hämtad: 2019-03-29].

Zavyalova, Kira; Stubbs, Jack och Neely Jason. ”Home Credit’s Russian bank suspends IT systems after cyber attack”. *Reuters*, 2107-06-28. https://www.reuters.com/article/us-cyber-attack-homecredit-russia/home-credits-russian-bank-suspends-it-systems-after-cyber-attack-idUSKBN19J10I [Hämtad: 2019-03-29].

Zinets, Natalia. ”Ukraine central bank warns of new cyber-attack risk”. *Reuters*, 2017-08-18. https://www.reuters.com/article/us-cyber-ukraine-banking-idUSKCN1AY0Y4 [Hämtad: 2019-03-27].

Почта Маркет [Pochta Market]. https://market.pochta.ru/ [Hämtad: 2019-02-06].

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se