FOI MEMO

Projekt/Project		Sidnr/Page no
Cyberoperationer		1 (8)
Projektnummer/Project no	Kund/Customer	
E72887	Försvarsmakten	
FoT-område		
Inget FoT-område		

Handläggare/Our reference	Datum/Date	Memo nummer/Number
David Lindahl	2020-06-03	FOI Memo 7434

IT Vulnerabilities in the healthcare system – the example of Wannacry and the cyberattack on the British National Health Service

David Lindahl, Birgitta Liljedahl och Annica Waleij

1 Introduction

The healthcare and social care sector, alongside resilient energy supply, food and water resources systems, information and telecommunications networks, the security and safety sector and financial services, are prioritised societal sectors by the Swedish Civil Contingencies Agency (MSB).[1,2]

Digitalisation in general and in the healthcare sector in particular offers opportunities as well as challenges regarding the rapid development of IT-infrastructure, Internet of Things (IoT) and new IT-based tools. One of the challenges is that increased dependencies on computer services increases the risks of cyberattacks affecting those services. Vulnerabilities in healthcare computer systems have been revealed in numerous ransomware[3] attacks over the years. More recent, the cyberattacks during the Covid-19 pandemic[4] are still ongoing.

The healthcare system might be exposed to several challenges beyond "business as usual" activities, with e.g. an aging population, welfare diseases, growing antibiotics resistance, vehicle accidents and a growing scepticism for vaccines. An epidemic outbreak of infectious disease might occur in parallel with natural or man-made disasters such as forest fires or chemical spills from an industrial accident, making the combined number of casualties overwhelming. A worst-case scenario include an antagonistic attack,[5] where chemical, biological or radiological (CBR) substances might be involved.

The healthcare sector is a vital strategic national resource critical for any form of mass casualty event, where the capacity threshold will be strained, potentially beyond normal capacity. Some, but far from all military organisations have organic healthcare capacity, and are hence subject to sharing healthcare with the civilian society.

Furthermore, even prior to the outbreak of SARS-CoV-2, the healthcare sector was one of the most targeted sectors for cyberattacks.[6] Cyberspace has also been added as an additional operations domain by e.g. Nato. Thus, there is a reason to look deeper into previous cyber-attacks with impact on the healthcare sector, to gain a better understanding of what challenges might lay ahead.[7] This report is one in a series of follow-up briefs regarding the conclusions made in the report "A wider perspective on CBRN related threats".[8]

2 Wannacry timeline

On Friday 12 May 2017, a lower activity period for the National Health Services (NHS), the Wannacry ransomware attack was launched. The first infection noted was logged at 07:44 UTC [9]

[1] Myndigheten för samhällsskydd och beredskap (2017) Nationell risk- och förmågebedömning 2017, april 2017.

[2] Similarly, Nato has identified seven baseline requirements for national resilience, where the ability to deal with mass casualties, in one requirement. See Justitiedepartementet (2017) Raminstruktion för det svenska civila beredskapsarbetet inom ramen för Nato/PFF, 2017-06-22. https://www.msb.se/Upload/Om%20MSB/Internationellt/Raminstruktion-2017.pdf

[3] *Ransomware* is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

[4] Lindahl, D. Liljedahl, B. Waleij, A. (2020) Cyberattacks in the healthcare sector during the first three months of the Covid-19 pandemic. FOI Memo 7062.

[5] SVT DIREKT 14.00h Covid-19 update April 3rd 2020 news public information by MSB regarding critical infrastructure and telecom in healthcare (SVT)

[6] Muresan, R. 2019. "Healthcare Continues to Be Prime Target for Cyber Attacks". Bitdefender Business Insights Blog post. 07 January 2019. https://businessinsights.bitdefender.com/healthcare-prime-target-for-cyber-attacks

[7] Waleij, A. Liljedahl, B. Börjegren, S. Lindahl, D. (2019) Vidare kontext för en CBRN-relaterad hotbild. FOI, Stockholm, Sweden, FOI-R--4781--SE, ISSN 1650-1942

[8] Waleij, A. Liljedahl, B. Börjegren, S. Lindahl, D. (2019) Vidare kontext för en CBRN-relaterad hotbild. FOI, Stockholm, Sweden, FOI-R--4781--SE, ISSN 1650-1942 https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4781--SE

[9] Universal coordinated time

when a host in south-east Asia attempted a DNS[10]-lookup for the command and control web address for the cyber weapon[11]. From there the weapon spread very quickly. The first communication from infected hosts in Latin America were logged at 08:16 UTC and Europe in 10:05 UTC[12].

By the end of the first day of spreading, it had infected more than 75 000 hosts in 99 countries[13]. Within two days, it had been detected in more than 150 countries, with some 230 000 hosts infected[14]. The spread of Wannacry was considerably slower than it might have been, however. The programmers behind Wannacry had included an emergency switch, which a UK security researcher discovered and activated late in the evening of Friday the 12th. This stopped the weapon from spreading over the internet, limiting it only to local networks.

In the United Kingdom, the National Health Services (NHS) reported that 80 of its 236 trusts were affected, five of which had to turn away even emergency patients. In addition to the trusts, 603 primary care facilities and other NHS organisations were affected.[15]

The activation of the emergency switch stopped further spread of the cyber-virus, however it did not stop the effects of the attack, since every infected machine had to be located, reinstalled and protected from reinfection from other machines on the local network.[16]

3 What is Wannacry?

Wannacry is a *worm,* a computer program that has the capability to connect to another computer and send a copy of itself to it. Wannacry accomplishes this by generating a list of random IP-addresses, and attempting to connect to all of them in turn[17] by using the *SMBv1 communication protocol.*[18]

If the remote computer is set to receive messages of this kind, Wannacry attempts to infect it. This is accomplished using the *Eternal Blue*-exploit.[19] Wannacry then sends the victim a copy of itself that is run on the victim machine. The copy can access any local networks the victim computer is connected to, and can spread to them in turn.

This double spread makes use of the fact that most computers today are connected both to the internet and local networks. All the infected machines try to infect a number of machines over the internet but not so many that Internet Service Providers (ISPs) will take notice. They will then spread new copies of the worm inside the local networks attempting to take control over as many hosts as possible as fast as possible. This combination of approaches allowed the worm to spread

[10] Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network

[11] SophosLabs (2017) WannaCry: the ransomware worm that didn't arrive on a phishing hook. 17 Maj 2017 https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/

[12] Einav, Y. (2017) Wannacry: Views from the DNS frontline. Akamai Security and Intelligence Research, May 15, 2017, https://blogs.akamai.com/sitr/2017/05/wannacry-views-from-the-dns-frontline.html?locale=en

[13] BBC News (2017) Cyber-attack: Europol says it was unprecedented in scale, 13 May 2017 https://www.bbc.com/news/world-europe-39907965

[14] Kaspersky (2017) What is WannaCry ransomware? https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[15] Smart, W. (2018) Lessons learned review of the WannaCry Ransomware Cyber Attack. London: National

[16] Health Service, 2018 s. 5 & s. 14. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learnedreview-wannacry-ransomware-cyber-attack-cio-review.pdf

[17] Naked Security (2017) WannaCry: the ransomware worm that didn't arrive on a phishing hook 17 May 2017, https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/

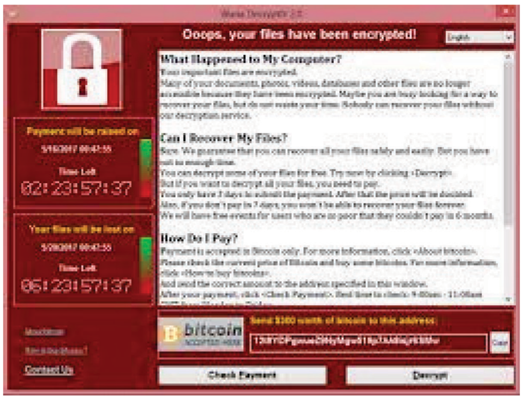
[18] Server Message Block Protocol (SMB protocol) is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network

[19] "Exploit" is the term for a program crafted to exploit a specific security vulnerability in a computer. In this case the attacking program sends a message deliberately deviating from the expected SMB standard. This causes the receiving computer program to malfunction which lets Wannacry send instructions to the computer, effectively remote controlling it [Microsoft Security Bulletin MS17-010].

faster, and confused responders. As the second stage attack only seemed to spread within local networks, many assumed the attack vector was through an email or a user that had clicked on a malicious link on a webpage.[20]

Once the phase spreading the worm to other computers is completed, Wannacry encrypts[21] the hard drives of the computer and displays a message demanding a ransom paid in Bitcoins to unlock the files. Menacingly, it displayed two timers that purports to show how long the victim has before the ransom is increased and (after seven days) the option to restore the files is lost forever.

This action leads to damage in several ways. First, it denies the user of the computer access to information stored on the computer, but also it denies the user access to services provided by other computers. This means that central services such as patient records databases or email services are no longer available.



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Figure 1. The Wannacry instruction screen

[20] Kaspersky (2017)

[21] Encryption is a process of altering information so it becomes unreadable without possession of a specific piece of information known as the *key*.

4 Impact on the NHS

Approximately one third of the 236 NHS Trusts were affected to the point of disruption of services, as well as around 600 other primary care and NHS organisations. Eight percent of the General Practitioners practices were also affected.[22]

Of the 80 Trusts affected to the point of disruption only 34 actually had computers attacked and shut down. The others were affected either by handling the overflow of patients from the other trusts or dealing with the loss of services such as electronic patient records and clinical information from service providers with systems directly affected by the cyberattack[23].

In total, 6 912 or approximately 1.2% of NHS England's first appointments were cancelled from the 12th to the 18th of May.[24] The estimated number for the whole of the UK is over 19 000[25]. No data has yet been officially published regarding the number of cancelled General Practitioner's (GP) appointments, nor on how many ambulances and patients were diverted from emergency clinics unable to receive patients. Nor is it currently known how many NHS organisations that could not access records or receive information because they shared data or systems with an infected trust but were not so severely affected that operations were disrupted.

1221 diagnostic systems were affected, which comes to around 1% of the NHS total. No data is currently available on how many non-diagnostic computers or system were affected.

According to the official investigations, no patients died or were seriously harmed by the attack.[26, 27] Since the attack began on a Friday, the weekend provided two days of rescheduling patient appointments, and with the addition of volunteers and improvisation 22 of the 27 stricken acute trusts managed to keep on treating patients.

5 Conclusions from the NHS handling of the Wannacry incident

Cyber hygiene was lacking

A security patch for the vulnerability used by Wannacry had been made available from Microsoft on March 14 for all the Microsoft operating systems that were still supported at that time[28]. The NHS had been warned in 2014 by the Department and Cabinet Office that it was essential that they had robust plans for migrating from the Windows-version XP that were about to be phased out from support by Microsoft by April 2015.[29] However, not only were security patches lacking from more modern machines despite having been available for weeks, but 4.7% of the devices run by NHS at

[22] Smart, W. (2018)
[23] Ibid
[24] Ibid
[25] National Audit Office (2018), Investigation: WannaCry cyber attack and the NHS, , https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
[26] Ibid
[27] Smart, W. (2018)
[28] Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2016
[29] National Audit Office (2018)

the time of the attack were still Windows XP-machines.[30] Even as late as July 2019 NHS had 2 300 machines still running Windows XP, an operating system so old it has not been supported since 2015.[31]

One reason for this situation is that medical technology such as MRI-scanners cannot easily be upgraded from one version of an operating system to another. In combination with the long service life of medical equipment this means that some equipment must effectively be quarantined behind security measures or removed from computer networks because they simply cannot be upgraded.

However, given that most infections struck unpatched Windows 7 machines the situation resulted at least in equal measure from a lack of a systematic and continuous IT security process operating in the organisations as from the difficulty of upgrading old Windows XP machines in the networks.[32]

Given the expected future development with more and more computers and digital equipment, this is a point that cannot be over-emphasized. The use of computerised equipment in the healthcare arena must be a life-cycle activity that takes into account software upgrades in all manner of equipment from dialysis machines to electronic patient journal systems to heart starters. In addition, there is an increased need for competence in IT security, in the procurement chain of any device, small or large, expensive or cheap, that might become a weak link and used to enable cyberattacks.

Incident preparations for Cyber emergencies were lacking

Responsibilities within and between the different organisations had not been hashed out beforehand. Preparations for handling digital support systems or diagnostic equipment failure had not been made, and no plans had been drawn up for establishing emergency communication or acquire emergency local technical assistance.[33]

Proactive activities are essential for handling a cyber-emergency. Establishing procedures, staffing incident teams and training personnel in proper response is as time consuming as training them for a conventional emergency.

6 Future areas of risk

In addition to the conclusions above there are several trends that indicate more trouble ahead. The increased levels of digitisation both in services and technical equipment open several potential risk areas.

Increased numbers and levels of unknown dependencies

The amount of information gathered, disseminated and analysed by the modern healthcare organisation is enormous. More and more, systems are automated so that for example a life support machine will send data to a central server for everyone to access as needed, and computers will note deviations and send alarms to doctor's handsets or a nurse station's monitors. This automation dramatically enhances the healthcare professionals' abilities to perform their jobs, but also means that many new access points are available for an attacker to exploit.

[30] NHS (2017) UPDATED Statement on reported NHS cyber-attack - 13 May, Last edited: 11 April 2018 5:39 pm, https://digital.nhs.uk/services/data-security-centre/data-security-centre-latest-news/updated-statement-on-reported-nhs-cyber-attack-13-may

[31] Trandall, S. (2019) NHS still running 2,300 PCs on Windows XP. Public Technology 16 July 2019. https://www.publictechnology.net/articles/news/nhs-still-running-2300-pcs-windows-xp

[32] Schwartz, M. J. (2017) WannaCry Ransomware Outbreak Spreads Worldwide. Bank info Security May 12, 2017, https://www.bankinfosecurity.com/telefonica-nhs-hit-by-massive-ransomware-attacks-a-9912

[33] National Audit Office (2018)

So an end user of for example a patient journal system might be affected by attacks or malfunctions that occur with several degrees of separation.

- A GP practice with only a few employees might not practice secure cyber routines, which lead to a cyber-weapon infecting their systems and subsequently affecting shared services such as database access to the patient journals system.

- An administrator might be the victim of a social engineering attack[34] which leads to their office workstations to become infected. Which in turn results in the local networks being overloaded with traffic causing the journal system to be inaccessible to the physicians although the service technically is online.

- The use of personal health-monitoring sensors is increasing. The equipment may send diagnostic and statistical data not only to the users, but also to vendors and healthcare providers. New equipment might be communicating (or have the capacity for communication) resulting in data leaks and attacker ingress, without the knowledge of the users[35, 36].

Decision support systems and Artificial Intelligence (AI)

The increasing number of computer systems designed to decrease the cognitive load of the healthcare professional can lead to a situation where a compromised software might be used in more subtle ways than the crude ransomware attacks, leading to long term damage and loss of confidence in the healthcare providers.

Already one software vendor has been exposed for receiving payments from a pharmaceutical company in exchange for making the software suggest the company’s products (opioid painkillers in treatment plans) even when such treatments did not reflect accepted medical standards[37]. An attacker gaining access to such software might be able to suggest medication that would be more directly harmful to patients. Other types of software control include cyber-physical interfaces, such as pacemakers or dialysis machines. As more and more trust is placed in the software controlling the systems, it becomes increasingly important to monitor the software to make sure it has not been manipulated.

This is especially relevant concerning machine learning systems and other kinds of AI, where the decision making is not based on rule sets that are human-readable and hence special software must be used to verify its functionality.

Software updates

The increasing number of systems with software will require security updates, not only in the application programs/apps but also to their operating systems. The Wannacry incident showed that many systems used in healthcare were not designed to be frequently updated, and even in the cases where updates were available, the organisation and routines to do so were lacking. This problem will

[34] In this context “*Social Engineering”* means the use of deception to manipulate victims into taking actions that seem reasonable but that divulges information to the attacker, or causes a vulnerability in a computer system. E. g. sending a virus infected email attachment in the hopes that the receiver will open it and infect their computer systems

[35] Ellen Klas, M. & Conarck, B. (2020) Thermometer company: Florida compares only to NYC in spike in fever data, March 20, 2020
https://www.miamiherald.com/news/coronavirus/article241372271.html

[36] Hsu, J. (2018) The Strava Heat Map and the End of Secrets. Wired Security, 29 January 2018
https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

[37] Quach, K. (2020) SF tech biz forks out $146m in fines, settlements after painkiller makers bribed it to design medical software that pushed opioids to patients. The register, 31 January 2020
https://www.theregister.co.uk/2020/01/31/practice_fusion_opioids/

most likely be exacerbated in the future when even more systems are digitized, especially in sectors, and parts of organisations that previously have not had experience with these issues. A particularly worrying prospect is attacks on the update supply chain. The same year as Wannacry, the NotPetya attack struck, using many of the same exploits but facilitating its initial spread by using the update service of the company M.E.Doc to send out a fake update of their software. This was accepted and run by almost all customers who then unwittingly also installed the malware on their systems[38, 39]. This kind of attack, given how many updates an organisation has to deal with on a weekly basis, risk placing organisations in a "Scylla and Charybdis"-dilemma where the choice is to wait with a patch install, and risk attack, or go ahead with a patch install, and risk another attack. It is therefore necessary that vendor updates can be authenticated, and that the vendor's security level is at least equal to the security level of the organisations trusting them.

7 Summary

The future use of digital systems will demand a great deal from the healthcare sector. In order to secure their digital systems against cyber threats a holistic approach with many layers of overlapping activities must be in place. Key concerns include, but are not limited to:

- The use of computerised equipment in the healthcare arena must be a life-cycle activity that takes into account software upgrades in all manner of equipment from dialysis machines to electronic patient journal systems to heart starters.
- Proactive activities are essential for handling a cyber-emergency. Establishing procedures, staffing incident teams and training personnel in proper response is as time consuming as training them for a conventional emergency.
- As more and more trust is placed in the software controlling the systems (e.g. AI), it becomes increasingly important to monitor the software to make sure it has not been manipulated.
- The increasing number of systems with software will require security updates, not only in the functional programs/apps but also to their operating systems.
- This problem will most likely be exacerbated in the future when even more systems are digitized, especially in sectors and parts of organisations that previously have not had experience with these issues. There is a need for increased competence in IT security in the procurement chain of any electronic devices that might become a weak link and enable cyberattacks.
- A particularly worrying prospect is attacks on the update supply chain.

[38] Microsoft (2017) New ransomware, old techniques: Petya adds worm capabilities, June 27, 2017 https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc

[39] Sattler, J (2017) Petya Ransomware FAQ: Known Knowns and Unknowns, FSecure 28 June 2017, https://blog.f-secure.com/petya-ransomware-faq-known-knowns-and-unknowns/