Sammanställning över utlärande spel med inriktning på cybersäkerhet

Sändlista/Distribution:

Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

1 Inledning

FOI har genom ett antal kursutvecklingsuppdrag från Myndigheten för samhällsskydd och beredskap (MSB) utvecklat lärande spel för användning inom medvetandehöjande och kunskapshöjande utbildningar inom cybersäkerhet.[1] Som en del i detta arbete har forskare vid FOI också kommit i kontakt med liknande initiativ från andra aktörer. I detta memo presenteras en översikt av de lärande spel som har identifierats inom ramen för dessa projekt.

[1] FOI-2018-126:26 resp. MSB 2018-03306 samt FOI-2020-1052:3 resp. MSB 2020-09820

2 Identifierade spel

Totalt har tolv lärande spel identifierats inom ramen för detta arbete. Läsaren bör dock notera att det inte har varit en huvudaktivitet inom något projekt att studera andras spel. Således är det troligen inte en komplett sammanställning och informationen om respektive spel är också relativt kortfattat.

2.1 <CMD> & <CTRL>

<CMD> & <CTRL> (utläses Command and Control) är ett kortspel som har utvecklats av FOI på uppdrag av MSB. Spelet är framtaget för att användas som en mer lättsam aktivitet på en cybersäkerhetskurs för myndighetschefer och ska vara underhållande och samtidigt utbildande. <CMD> & <CTRL> är framtaget för att passa grupper på två till åtta spelare men antalet kort justeras baserat på antalet spelare och önskad speltid.

I en kortlek finns fyra olika typer av kort, varav en delmängd visas i Figur 1. *Tillgångar* är skyddsvärda system som deltagarna ska samla *Skyddsåtgärder* för att skydda mot *Incidenter*. Spelet spelas medsols i omgångar och varje tur väljer deltagarna mellan fem olika aktiviteter. Målet är att samla skyddsåtgärder för att skydda tillgångar och för varje tillgång behövs mellan två och fem olika skyddsåtgärder. När en deltagare har samlat alla skyddsåtgärder som behövs, läggs dessa ned på bordet och ger deltagaren poäng. *Jokrar* används för att förändra konsekvenserna när en incident spelas.

Figur 1: En översikt över de fyra kategorierna av kort som ingår i <CMD> & <CTRL>, tillgångar, skyddsåtgärder, incidenter och jokrar.

Spelets lärande moment består i första hand av de diskussioner som möjliggörs av spelkorten, men det kan vara en fördel att använda en spelledare för att ytterligare förstärka lärandet. En viktig förutsättning vid framtagandet har varit att spelet ska vara enkelt att förstå. Erfarenheter från de gånger som spelet har använts visar på att deltagarna behöver mindre än tio minuter på sig för att lära sig de grundläggande dragen i spelet. <CMD> & <CTRL> presenteras mer utförligt i ett separat FOI Memo.[2]

2.2 Cyber Card Game

Cyber Card Game är ett kortspel som har utvecklats av den brittiska myndigheten Defence Science and Technology Laboratory (DSTL).[3] Enligt DSTL är spelet inriktat på att hjälpa spelarna att förstå och identifiera metoder för angrepp mot industriella och kommersiella system. Spelet är tänkt att ledas av en erfaren spelledare, finns i flera versioner och kan spelas igenom på cirka två timmar.[4] En kommersiell version av spelet utvecklas av Coruscant Productions.[5]

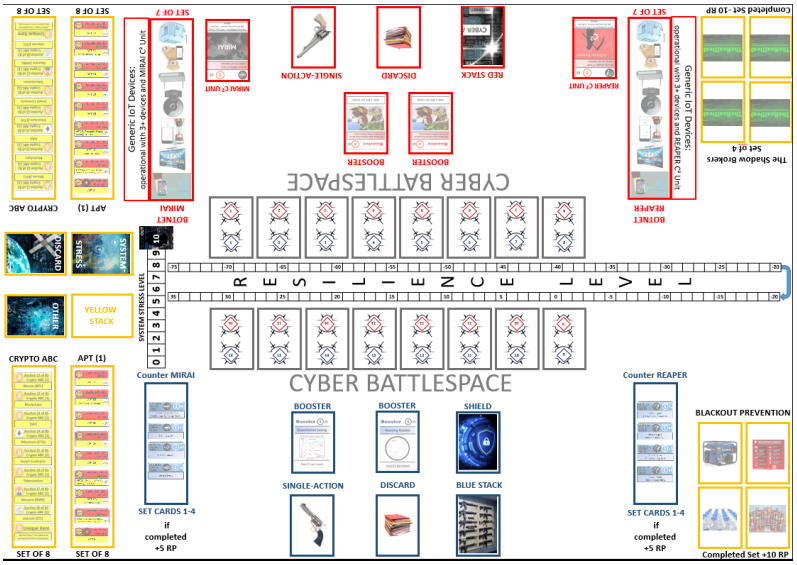
2.3 Cyber resilience card game

Cyber resilience card game (CRCG) är ett spel som är utvecklat inom ramen för NATO:s forskningsverksamhet av SAS-129 Gamification of Cyber Defence/Resilience.[6] Spelet finns beskrivet i en mastersuppsats publicerad 2020.[7]

I spelet finns tre roller, angripare (Röd), försvarare (Blå) och bank/spelledare (Gul). Den gula spelaren är ett valfritt tillval. De spelregler som finns publicerade är något sparsamt dokumenterade men i princip spelas spelet i omgångar där angriparen börjar. Under varje omgång placerar respektive spelare ett eller flera spelkort på spelplanen som visas i Figur 2. Dessa ”köps” in för olika valutor, bitcoin för angriparen och dollar för försvararen. Båda spelarna börjar med 20 enheter av respektive valuta och tjänar ytterligare en per omgång. Angriparens mål är att minska försvararens *Resilience points (RP)* genom att lägga ut olika angreppskort på spelplanen. När angriparen har spelat sin omgång är det försvararens tur att lägga ut ett eller flera spelkort på spelplanen för att höja sina RP.

Spelet pågår tills angriparen antingen har orsakat ett avbrott eller när försvararen har slut på sina kort. Försvararen vinner om denne har en summa av RP som överstiger noll. I annat fall vinner angriparen.

[2] Gustafsson (2021)
[3] Gov.uk (2018)
[4] DSTL (2018)
[5] Gov.uk (2018)
[6] Kodalle (2020a)
[7] Kodalle (2020b)



Figur 2: Spelplanen som används för CRCG. Denna trycks i formatet A0.

Den tredje spelaren är valfri och kan närmast ses som en spelledare. Denne har en gul kortlek tillgänglig som innehåller kort indelade i tre kategorier. Den första kategorin i den gula kortleken kan stärka både angriparen och försvararen och dessa kan köpas via ett auktionsförfarande. Den andra kategorin av kort är bara möjliga att köpa för den ena parten. Den tredje kategorin innehåller händelser i spelet som påverkar spelets förlopp. Dessa kan inte köpas av någon spelare. Om någon tredje spelare/roll inte är tillgänglig, kan de gula korten istället dras ur en hög vilket gör det möjligt att spela CRCG på två eller tre spelare.

På kortens baksida finns det QR-koder som innehåller information om kortens bakgrund. Det är tydligt att utvecklarna har lagt mycket tid på spelets innehåll.

2.4 CYNIC

CYNIC är ett kortspel för att träna informationssäkerhet[8] och har utvecklats av Luleå Universitet inom ramen för projektet Cyber security in Innovation and Business Communication (CYNIC)[9]. Syftet är att öka deltagarnas förståelse för informationssäkerhet och spelet riktar sig i första hand till små och medelstora företag. I spelet, som beskrivs i ett YouTube-klipp[10], har varje spelare en hand kort som representerar fyra roller markerade med fyra olika färger som syns i Figur 3. Spelet går ut på att spela skyddsåtgärder på de egna rollerna samt hot på de andras roller. Det är tillåtet att samarbeta med andra spelare, till exempel genom att lägga skyddsåtgärder på deras roller.

[8] CYNIC (2020a)
[9] CYNIC (2020b)
[10] https://www.youtube.com/watch?v=7GSXppFjruc&feature=youtu.be

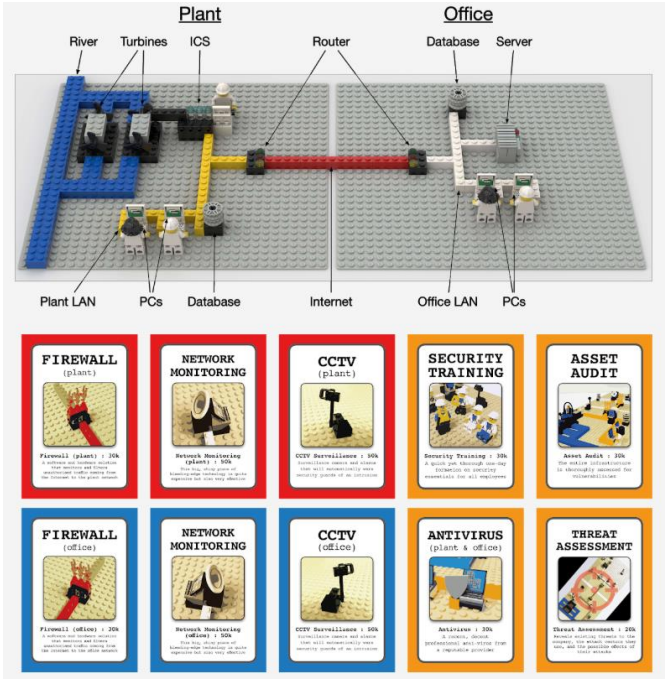
Figur 3: De fyra färgerna representerar de fyra roller som spelarna kan ha. Bild: Luleå tekniska universitet (2019)

Spelet sker i omgångar där varje spelare i tur och ordning placerar skyddsåtgärder eller hot. Spelkorten finns på svenska och på engelska.

2.5 Decisions & Disruptions

Decisions & Disruptions är ett spel som har utvecklats av ett forskarlag vid Cyber Security Group på Bristol universitet. Syftet är att deltagarna ska hantera säkerheten i en mindre organisation som arbetar med kritisk infrastruktur.[11] Spelet är avsett för mellan fem och åtta deltagare plus en spelledare. Deltagarna arbetar med generiska skyddsmetoder. För att illustrera förloppet används en legomodell som visas i Figur 4. Under spelets gång ska deltagarna använda en begränsad budget för att prioritera en uppsättning olika skyddsåtgärder i sin organisation. Spelet genomförs i fyra omgångar och avslutas med att spelledaren går igenom de angrepp som har drabbat företaget.

[11] Frey et al. (2018)



Figur 4: Illustration över spelplanen som byggs i Lego samt de skyddsåtgärder som deltagarna kan implementera. Bild: Decisions & disruptions (2020)

Skaparna av Decisions & Disruptions använder spelet i sin forskning för att se hur olika grupper hanterar säkerhetsproblemen. Allt material för spelet finns tillgängligt på internet och det är möjligt att köpa in egna legouppsättningar motsvarande dem som används i spelet.[12]

2.6 Elevation of Privilege

Elevation of Privilege (EoP) är ett spel som har utvecklats av Adam Shostack på Microsoft. Syftet med spelet är att på ett lättillgängligt sätt lära utvecklare grunderna i mjukvaru-fokuserad hotmodellering och på så sätt minska behovet av att dessa aktiviteter alltid genomförs av säkerhetsexperter.[13] EoP är avsett för 3–5 spelare och består av en kortlek med 74 spelkort samt tio kort med instruktioner. Spelkorten är uppdelade i sex serier med hotkategorierna Spoofing, Tampering, Repudiation, Information disclosure, Denial of service och Elevation of privileges (namnen återges på engelska för att inte betydelsen ska förändras) i enlighet med Figur 5. Fyra serier innehåller kort med värdet 2 till 10 samt knekt till äss som i en vanlig kortlek men de två sista innehåller färre kort då skaparna inte kom på fler kort.[14] Spelet går därefter ut på att deltagarna i tur och ordning spelar ut ett kort och den som lägger det högsta kortet i en serie vinner sticket. Flest vunna stick i slutet av spelet har vunnit. Serien Elevation of privileges är trumf och slår alltid över övriga kort.

[12] Decisions & disruptions (2020)
[13] Shostack (2014)
[14] Ibid.

Figur 5: Elevation of privileges innehåller sex serier med hotkategorier. Dessa används för att spela ett kortspel som liknar första fasen i Skitgubbe där deltagarna ska plocka stick genom att lägga det högsta kortet.

Elevation of privileges delades initialt ut av Microsoft och finns fortfarande tillgängligt för nedladdning via deras hemsida[15].

2.7 FOI SI3S

FOI SI3S är ett spel som tagits fram av FOI som en del av kursen *Påbyggnadskurs Säkerhet i industriella informations- och styrsystem (PK-SI3S)* men som saknar eget namn. Kursens mål är att drifttekniker som arbetar med samhällsviktiga industriella informations- och styrsystem ska få fördjupad kunskap om de skyddsåtgärder som används inom cybersäkerhet. Pedagogiken är uppdelad i föreläsningar, laborationspass och en övning där spelet används för att ge deltagarna möjlighet att applicera den kunskap de fått från övriga moment.[16]

Spelet leds av en spelledare och går ut på att deltagarna i lag skall arbeta för att höja skyddsnivån i en fiktiv IT-miljö hos ett företag. Lagen arbetar med en spelplan med ikoner för olika system och kan varje omgång köpa in skyddsåtgärder eller flytta system. Spelplan, ikoner och skyddsåtgärder för scenariot Näverheat AB visas i Figur 6. Varje lag har olika scenarier och måste analysera och prioritera skyddsåtgärder baserat verksamhetens behov av konfidentialitet och tillgänglighet. Efter fyra spelomgångar kommer spelledningen att spela upp ett antal slumpvis utvalda hot som kan leda till konsekvenser för lagen.

[15] Microsoft (2021)
[16] Gustafsson (2019)

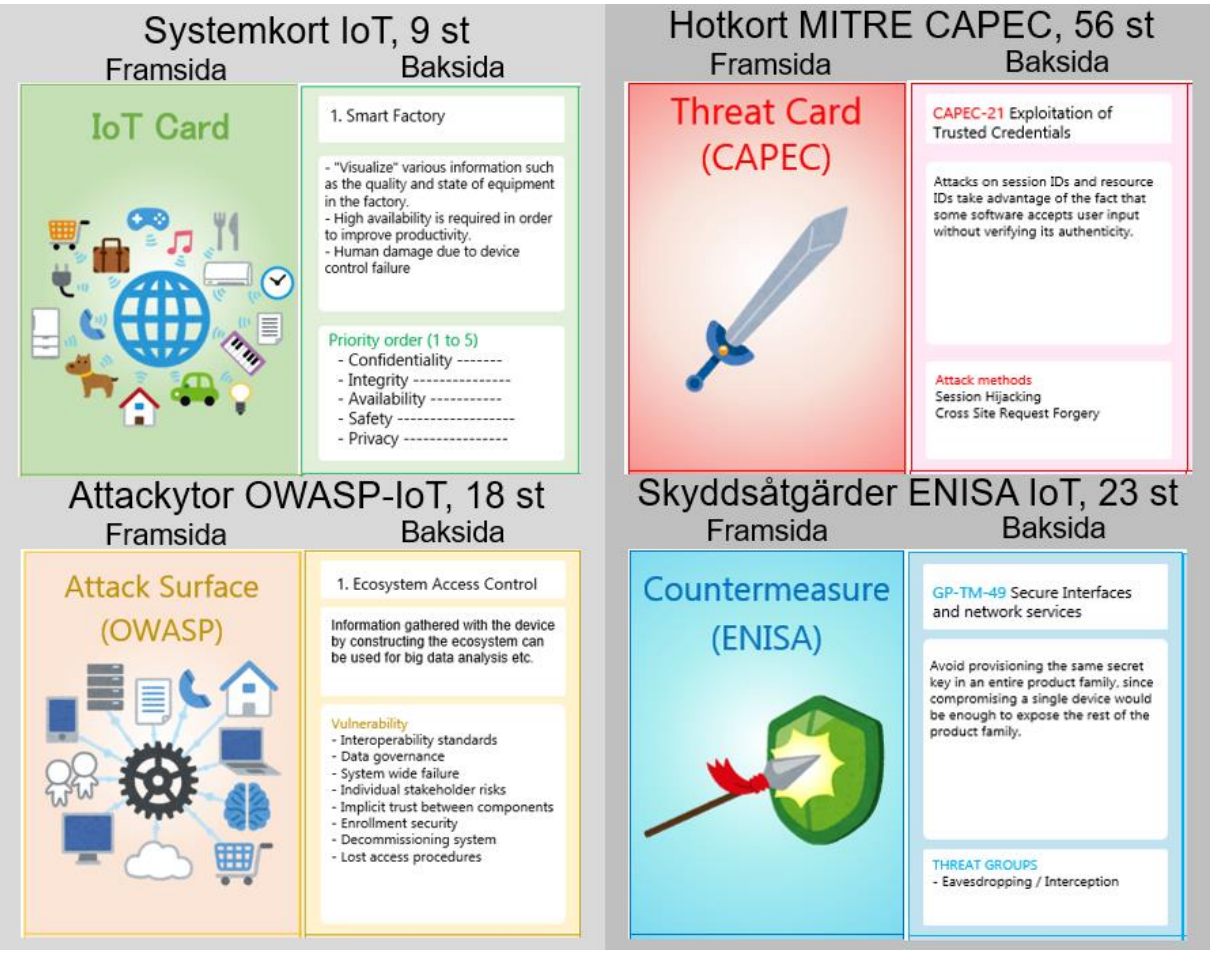
Figur 6: Spelplanen med tillhörande ikoner, skyddsåtgärder och scenario som används under övningen. Spelplanen innehåller fält där deltagarna kan fylla i sin progress.

En tidig version av spelet finns beskriven i FOI Memo 6757[17]. Spelet utvecklas dock kontinuerligt baserat på spelledarnas erfarenheter och deltagarnas utvärderingar efter varje genomförande. Detta har lett till en förenklad spelmotor och förtydligat gränssnitt av vilka delar beskrivs i FOI Memo 6988[18]. Idag används fyra olika scenarier och spelet genomförs med två till fyra lag med tre till sex deltagare per lag.

2.8 IoT-Poly

Secu-One är ett kortbaserat spel utvecklat vid Nara Institute of Science and Technology, Laboratory för Cyber Resilience i Japan[19]. Syftet är att deltagarna ska lära sig om hot och skyddsåtgärder med fokus på IoT och industriella informations- och styrsystem genom att utföra en riskanalys för ett fiktivt system. I spelet används fyra olika typer av kort i enlighet med Figur 7. Spelet inleds med att sammanlagt tio Hotkort och kort med Skyddsåtgärder delas ut till deltagarna. Därefter dras ett Systemkort som används tillsammans med en skiss för att ge deltagarna ett scenario att utgå ifrån. Det dras också ett kort med Attackytor som beskriver vilken typ av angrepp som systemet utsätts för. Varje deltagare skall baserat på detta välja ett hotkort varpå gruppen tillsammans värderar vilket hotkort som är mest allvarligt. Därefter väljer varje deltagare en eller flera kort med skyddsåtgärder som kan hantera hotet. Diskussionen mellan deltagarna är således en viktig del av lärandet.

[17] Westerdahl (2019a)
[18] Westerdahl (2019b)
[19] Omiya, Fall & Kadobayashi (2019)



Figur 7: I IoT-Poly används fyra typer av kort enligt figuren. Diskussionen sker baserat på ett systemkort och deltagarna leds genom processen at värdera säkerheten med hjälp av de tre övriga korttyperna.

En styrka med IoT-Poly är att de forskare som har utvecklat spelet har utgått från etablerade ramverk för att identifiera attackytor[20], hot[21] och skyddsåtgärder[22]. Spelet erbjuder däremot inget stöd för att identifiera attackytor, hot eller för att bedöma vilka skyddsåtgärder som hjälper mot respektive angrepp. Detta sker istället genom den diskussion som deltagarna har, möjligen med stöd av en spelledare.[23] Underlag för att framställa en egen kortlek och spelregler finns tillgängliga på GitHub.[24]

2.9 Kaspersky Interactive Protection Simulation

Spelet *Kaspersky Interactive Protection Simulation* (KIPS) är skapat av säkerhetsföretaget Kaspersky och går ut på att deltagarna skall skydda en verksamhet och hantera en serie händelser genom att fatta rätt beslut. De har en begränsad budget och tid så de måste

[20] OWASP IoT (2021)
[21] MITRE (2007)
[22] ENISA (2017)
[23] Nara Institute of Science and Technology (2019a)
[24] https://github.com/nabetan/IoT-Poly_En

balansera teknik, ekonomi och säkerhet. [25] Spelet är en hybrid mellan ett brädspel och ett datoriserat spel i enlighet med Figur 8. Brädspelskomponenterna inkluderar en spelplan och en uppsättning kort som beskriver företaget, dess miljö och deras system. Datoriseringen inkluderar en app på en iPad där deltagarna registrerar sina val och en serverbaserad mjukvara som används för att hålla reda på poäng och för att anpassa scenariot baserat på deltagarnas val.

Varje omgång inträffar nya händelser och deltagarnas val påverkar spelets scenario. Det finns en mekanism i spelet som bygger på att olika lag tävlar mot varandra genom att jämföra hur mycket pengar varje lag tjänar eller förlorar. Vid tiden få detta memo skrevs fanns sju grundscenarier för KIPS, *Corporation, Bank, Oil & Gas, Local Public Administration, Power Station or Water Plant, Transportation,* samt *Petrochemical industry*. [26] Namnen återges på engelska eftersom en översättning kan påverka tolkningen av vilka grundscenarier som finns.

Figur 8: Deltagarnas vy av Kaspersky Interactive Protection Simulation, i detta fall grundscenariot Power Station or Water Plant. Bild: www.helpnetsecurity.com

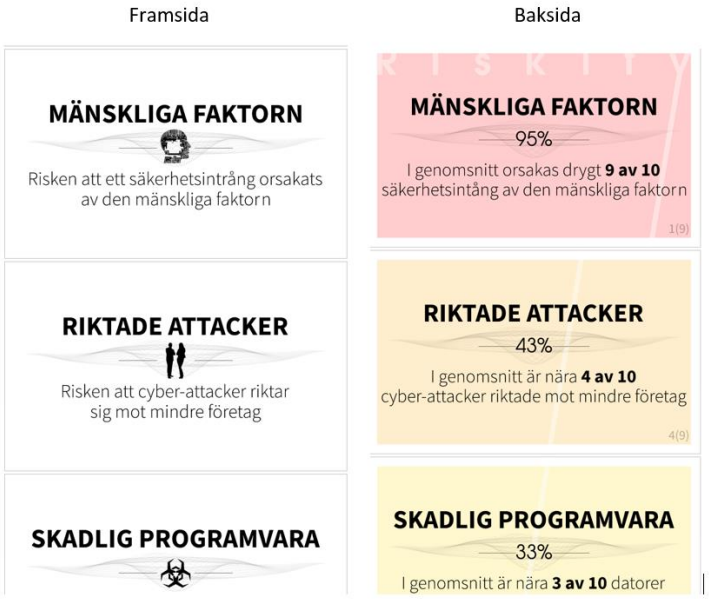
Spelet tar ungefär 2–3 timmar att spela och bedöms hålla mycket god kvalité. Kaspersky har ett upplägg där certifierade företag får genomföra spelet.

2.10 Riskify

Riskify är ett enklare kortspel som har utvecklats av Martin Lundgren[27] vid Luleå Universitet inom ramen för projektet Cyber security in Innovation and Business Communication (CYNIC)[28]. Syftet är att öka deltagarnas riskmedvetenhet och spelet består av nio

[25] Kasperskry (2019)
[26] Ibid.
[27] CYNIC (2020c)
[28] CYNIC (2020b)

dubbelsidiga spelkort enligt Figur 9. På framsidan beskrivs en risk och på baksidan presenteras sannolikheten för risken. Utan att titt på baksidan ska deltagarna placera korten i ordning, från det de bedömer ha lägst risk till högst risk. När deltagarna är överens om ordningen, vänder man på korten och får då se hur det faktiskt förhåller sig.



Figur 9: Fram- och baksida på tre av de kort som finns i spelet Riskify.

För närvarande innehåller Riskify nio spelkort, fem relaterar till cybersäkerhet och fyra relaterar till andra risker. Det är oklart hur lång tid en spelomgång tar men det går säkert att anpassa baserat på antalet deltagare och syfte med spelet. När deltagarna väl har spelat en gång, är det inte möjligt att återanvända samma spelkort på samma deltagare i och med att spelmotorn bygger på att dessa inte känner till det som står på kortens baksida.

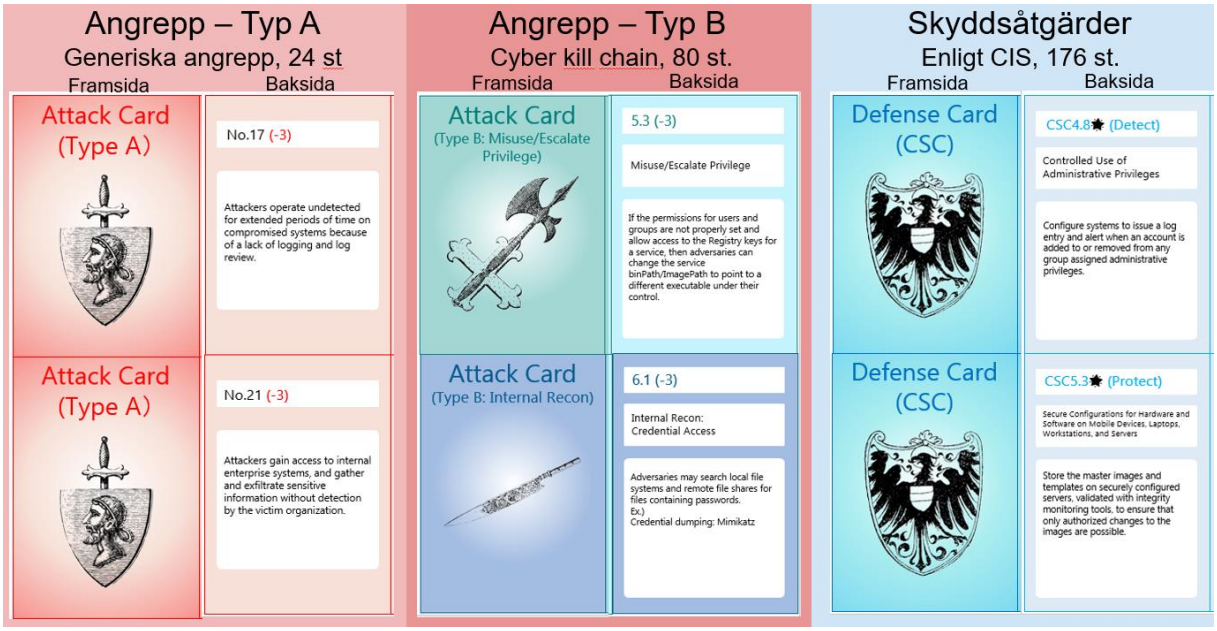
2.11 Secu-One

Secu-One är ett kortbaserat spel utvecklat vid Nara Institute of Science and Technology, Laboratory för Cyber Resilience i Japan[29]. Syftet är att deltagarna ska lära sig vilka skyddsåtgärder som är effektiva mot olika typer av angrepp. I spelet används två olika typer av kort, en för angrepp och en för skyddsåtgärder. Angreppskorten finns i Typ A och Typ B i enlighet med Figur 10.

Underlag för att framställa en egen kortlek och spelregler finns tillgängliga på GitHub.[30] Varje deltagare spelar med en egen uppsättning kort och i spelets inledning får varje deltagare tio kort med skyddsåtgärder.[31] Därefter sker en spelomgång genom att en spelledare drar ett angreppskort och deltagarna ska då lägga fram ett eller flera kort med skyddsåtgärder som de anser hjälper mot angreppet. De ska också förklara på vilket sätt det hjälper. Därefter ges

[29] Omiya, T & Kadobayashi, Y. (2019)
[30] https://github.com/nabetan/Secu-One_En
[31] Nara Institute of Science and Technology (2019b)

deltagarna poäng baserat på hur snabbt de fick fram en skyddsåtgärd och hur bra dessa bedöms vara.[32]



Figur 10: I Secu-One används skyddsåtgärder baserade på CIS för att skydda mot olika typer av angrepp. Det finns två uppsättningar angreppskort, ett baserat på generiska angrepp och ett baserat på Cyber kill chain.

De forskare som har utvecklat Secu-One har utgått från de så kallade CIS-kontrollerna från Center for Internet Security.[33] Angreppskorten finns i två versioner, en som baseras på Lockheed Cyber kill chain samt en uppsättning med generiska angrepp.[34] Spelet erbjuder inget stöd för att bedöma vilka skyddsåtgärder som hjälper mot respektive angrepp utan det är något som deltagarna antingen ska komma fram till i sina diskussioner eller som bestäms av en spelledare.[35]

2.12 Targeted attack

Targeted attack är ett incidenthanteringsspel som har utvecklats av säkerhetsföretaget Trend Micro.[36] Spelet är ett brädspel i enlighet med Figur 11 och riktar sig till lag med mellan 4–7 deltagare och anges ta 1 timme och 40 minuter att spela.[37] Det finns i fyra olika versioner, standard, ekonomi, medicinsk och universitet.[38]

Alla spelare ingår i samma lag och tilldelas olika roller hos ett fiktivt företag. Därefter dras kort med olika incidenter och laget ska tillsammans diskutera utredningsmetoder, återhämtningsmetoder och kommunikationsplaner, allt för att hantera den incident som korten visar.[39] Varje deltagare ska agera i enlighet med den roll som de tilldelats.

[32] Nara Institute of Science and Technology (2019b)
[33] Omiya & Kadobayashi (2019)
[34] Ibid.
[35] Nara Institute of Science and Technology (2019b)
[36] Studio Arcana (2016)
[37] Trend Micro (2016a)
[38] Trend Micro (2016b)
[39] Trend Micro (2016a)

Figur 11: Targeted attack är ett brädspel med fokus på incidenthantering. Som synes av bilden är spelet på japanska och det har inte gått att hitta en engelsk version. Bild: Trend Micro (2016a)

Det är möjligt att ladda ned spelet från Trend Micro[40] men informationen om spelet är i övrigt väldigt knapphändig då det mesta av materialet, inklusive spelkort och spelplan endast verkar finnas på japanska.

[40] https://resources.trendmicro.com/jp-docdownload-form-m057-web-incidentboardgamestandard.html?_ga=2.103507072.1003713196.1610375972-186516629.1609947606

3 Slutsatser

Utlärande spel utvecklas av både myndigheter, akademiska lärosäten och kommersiella företag. Gemensamt för flertalet av de spel som presenteras i detta memo är att de har tagits fram för att på ett underhållande sätt lära deltagarna cybersäkerhet. I de flesta fall är den tänkta målgruppen personer som har begränsad kunskap inom området men det finns flera exempel på spel som även vänder sig mot tekniker. Ett intressant exempel är Evolution of privileges som skaparen hävdar kan användas för att genomföra en hotanalys på ett riktigt system samt Targeted attack som kan användas för att identifiera brister i den egna incidenthanteringen. I samtliga fall beskriver skaparna av respektive spel att dessa har upplevts positivt av deltagarna och de beskrivs som ett engagerande och lättillgängligt sätt att lära sig cybersäkerhet.

En annan inriktning som kan vara intressant för framtida forskning vid FOI är att undersöka hur akademiska lärosäten har använd utlärande spel för att bedriva forskning såsom är fallet med Decisions & Disruptions, IoT-Poly och Secu-One. I förekommande fall har studierna fokuserad på hur deltagare med olika kunskapsnivåer inom cybersäkerhet väljer att agera inför olika problem. Inga studier har dock identifierats på hur utlärande spel påverkar deltagarnas förståelse för eller kompetens inom cybersäkerhetsområdet på sikt.

4 Källor

CYNIC (2020a), *Game – Cynic Project*. https://www.cynic.se/training/game/ [2020-12-22]

CYNIC (2020b), *About – Cynic Project*. https://www.cynic.se/about/ [2020-12-22]

CYNIC (2020c), *Riskify – Cynic Project*. https://www.cynic.se/training/riskify/ [2020-12-22]

Decisions & disruptions (2020), *Decisions & Disruptions.* Lancaster University, CC-BY-NC https://www.decisions-disruptions.org/ [2020-12-22]

DSTL (2018). *Easy_Access_IP_Cyber_Card_Game. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/712628/Easy_Access_IP_Cyber_Card_Game.pdf [2021-01-11]*

ENISA (2017). *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*. European Union Agency For Network And Information Security. ISBN: 978-92-9204-236-3, DOI: 10.2824/03228

Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M. & Naqvi, S. A. (2018) *The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game* ICSE 2018 Proceedings of the 40th International Conference on Software Engineering

Gov.uk (2018). *Scientists move away from the keyboard to beat cyber attackers at their own game.* https://www.gov.uk/government/news/scientists-move-away-from-the-keyboard-to-beat-cyber-attackers-at-their-own-game [2021-01-11]

Gustafsson, T. (2019). *SI3S-fortsättningskurs – pedagogisk plattform för övningen* (FOI Memo 6684) Stockholm: Totalförsvarets forskningsinstitut (FOI).

Gustafsson, T. (2021). *Spelregler CMD och CTRL* (FOI Memo 7473). Stockholm: Totalförsvarets forskningsinstitut (FOI).

Gustafsson, T. & Westerdahl, L. (2019) *Using serious gaming to train operators of critical infrastructure: an Industry/Experience report* CRITIS 2019, Proceedings of the 14th International Conference.

Hutchins, E., Cloppert, M. & Amin, R. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Leading Issues in Information Warfare & Security Research.

Kaspersky (2019), *Kaspersky Interactive Protection Simulation.* https://media.kaspersky.com/en/business-security/enterprise/KL_SA_KIPS_overview_A4_Eng_web.pdf [2020-12-22]

Kodalle, T. (2020a), *Cyber Wargaming on the Technical/Tactical Level: The Cyber Recilience Card Game (CRCG)* European Conference on Cyber Warefare and Security, ECCWS 2020

Kodalle, T. (2020b), *Gamification of Cyber Defence/Resilience at the Bundeswehr Command and Staff College (BwCSC)* Master Thesis, Helmut Schmidt Universität, Hamburg

Luleå tekniska universitetet (2019), *CYNIC – Spelregler*. https://www.youtube.com/watch?v=7GSXppFjruc [2020-12-22]

Microsoft (2021), *Download Elevation of Privilege (EoP) Threat Modeling Card Game from Official Microsoft Download Center*. https://www.microsoft.com/en-us/download/details.aspx?id=20303 [2021-01-11]

MITRE (2007). *CAPEC - A Community Resource for Identifying and Understanding Attacks*. https://capec.mitre.org/ [2021-01-06].

Nara Institute of Science and Technology (2019a). *IoT-Poly Game Manual Ver.1* Nara Institute of Science and Technology, Laboratory for Cyber Resilience

Nara Institute of Science and Technology (2019b). *Secure-One Game Manual Ver.1* Nara Institute of Science and Technology, Laboratory for Cyber Resilience

Omiya, T & Kadobayashi, Y. (2019), *Secu-One: A Proposal of Cyber Security Exercise Tool for Improving Security Management Skill.* ICIET 2019: Proceedings of the 2019 7th International Conference on Information and Education Technology. 259-268. 10.1145/3323771.3323792

Omiya, T., Fall, D. & Kadobayashi, Y. (2019). IoT-Poly: An IoT Security Game Practice Tool for Learners Motivation and Skills Acquisition. Koli Calling '19: Proceedings of the 19th Koli Calling International Conference on Computing Education Research. 1-10. 10.1145/3364510.3364519.

OWASP IoT (2021). *The OWASP Internet of Things Project*. https://owasp.org/www-project-internet-of-things/#tab=IoT_Attack_Surface_Areas. The OWASP Foundation [2021-01-06]

Shostack, A. (2014). *Elevation of Privilege: Drawing Developers into Threat Modeling*. USENIX - Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)

Studio Arcana (2016). *We actually played the Targeted Attack Board Game by Trend Micro #sa_study | BLOG | 株式会社スタジオ・アルカナ*. https://www.s-arcana.co.jp/blog/2016/12/01/3424 [2021-01-11]

Trend Micro (2016a). *Incident response board game: Stärk din organisations lyhördhet genom simulerad utbildning av säkerhetsincidenter*. https://resources.trendmicro.com/jp-docdownload-form-m057-web-incidentboardgamestandard.html?_ga=2.103507072.1003713196.1610375972-186516629.1609947606 [2021-01-11]

Trend Micro (2016b). *法人向けセキュリティ教育・学習コンテンツ*. https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/learning.html [2021-01-11]

Westerdahl, L. (2019a). *Föreläsningsmodul: Övningsupplägg* (FOI Memo 6757) Stockholm: Totalförsvarets forskningsinstitut (FOI).

Westerdahl, L. (2019b). *Uppdaterat kursunderlag: Påbyggnadskurs SI3S* (FOI Memo 6988) Stockholm: Totalförsvarets forskningsinstitut (FOI).