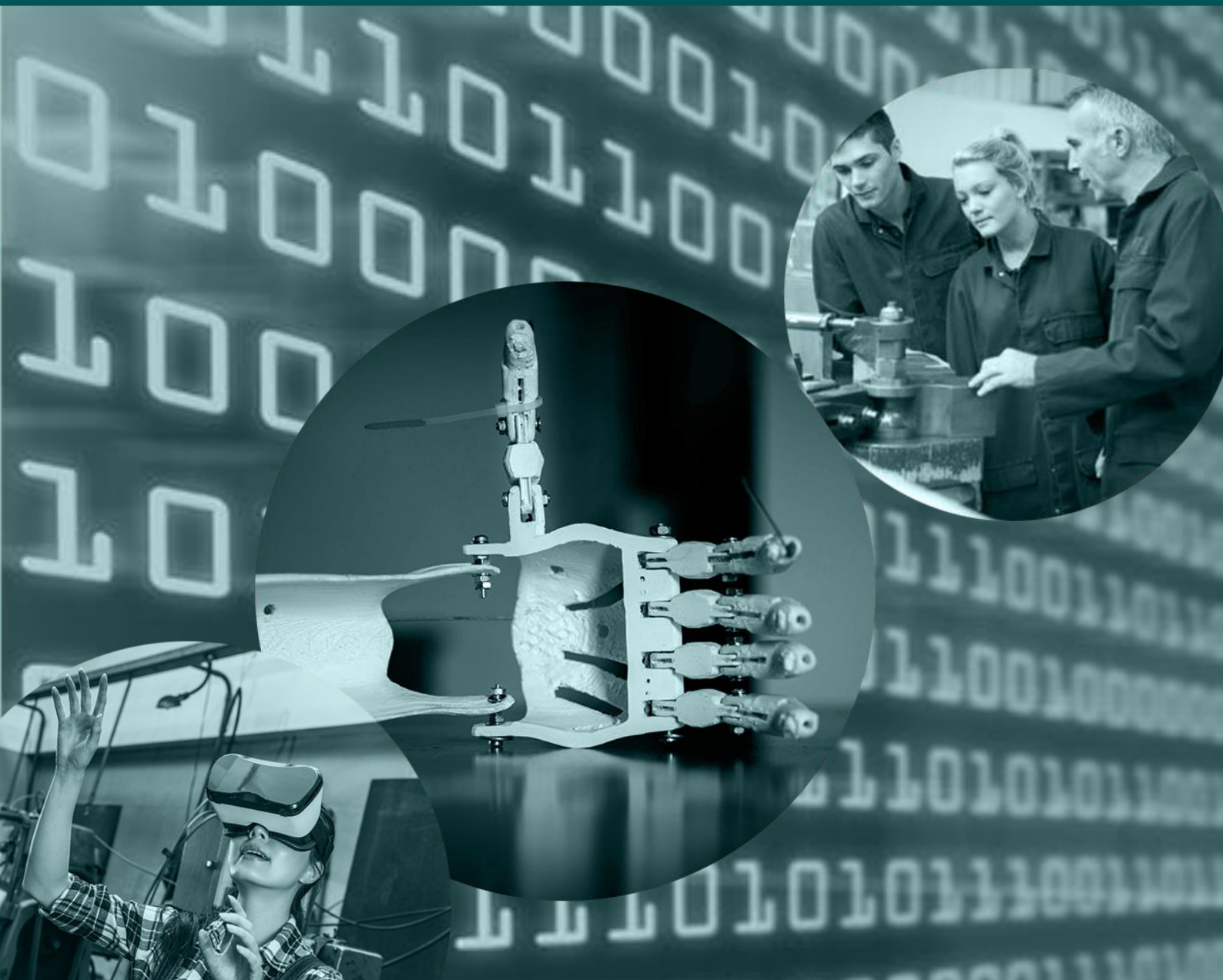
SpionageTesten 2.0

AFRAPPORTERING

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation



Indledning

CERTA har med støtte fra Industriens Fond og i et samarbejde med webbureauet AdResult lavet en relancering af SpionageTesten. Danske virksomheder er udsat for industrispionage mod deres aktiviteter og viden – og dermed dansk erhvervslivs konkurrenceevne. Samtidig er det imidlertid et område med mange mørketal, da den enkelte virksomhed ikke har en umiddelbar interesse i at blotlægge angreb og angrebsforsøg, da det kan være med til at fremstille virksomheden som sårbar og dermed påvirke virksomhedens troværdighed.

Siden lanceringen af SpionageTesten i 2016 er truslen fra f.eks. CEO-fraud, credential theft og ransomware-angreb vokset, ligesom blandt andet PET peger på, at insidertruslen fortsat er stor, men mindre belyst i åbne medier. Dette er alvorligt også for de små og mellemstore produktionsvirksomheder, der skal beskytte deres produktion, markedsandele og arbejdspladser.

SpionageTestens overordnede formål er fortsat at klæde virksomheder bedre på til at imødegå industrispionage. Målet er således dels at give konkrete løsningsforslag til den enkelte virksomhed, dels at øge bevidstheden om spionage og vigtigheden af gennemarbejdede sikkerhedstiltag – fysiske, digitale, kulturelle og ledelsesmæssige. SpionageTesten er fortsat et gratis og operativt orienteret værktøj.

Relanceringsarbejdet har været udført under følgende hovedpunkter:

- Opdatering af trusselsbillede
- Gennemgang og revision af spørgsmål, værdisætninger og sammenhænge
- Opdatering af links og materialesamling
- Formidling.

Aktiviteter og Leverancer

Arbejdet med relancering af SpionageTesten har været udført under fire hovedpunkter, der bliver gennemgået i detaljer i det følgende.

a. Opdatering af trusselsbillede

Der er udarbejdet en rapport til internt brug under overskriften Opdatering af trusselsbilledet – industrispionage. Her peges på, at mens analyser viser, at antallet af spionageangreb er stigende, og at produktionsvirksomheder er udsatte, så er det ikke en trussel, som virksomhederne nødvendigvis vurderer til at være sandsynlig. Det peger altså i retning af, at virksomhedernes risikobevidsthed ikke afspejler det faktiske trusselsbillede.

Insidertruslen bliver fremhævet som en af de trusler, der ofte overses. Det handler grundlæggende om, at medarbejdere af forskellige årsager kan udgøre en risiko for virksomheden ved aktivt eller utilsigtet at være det led, der gør, at erhvervskritisk information kommer i hænderne på de forkerte. Det kræver ikke nødvendigvis avancerede metoder at bedrive spionage. Det kan være alt fra en smartphone, der ligger på mødebordet og optager, til fysisk kopiering af dokumenter og download af materialer.

Der er stor bevågenhed på cyberangreb og deres betydning for også danske virksomheder. Ifølge Forsvarets Efterretningstjeneste så er truslen fra cyberspionage meget høj. Social engineering er et fænomen, der har fået mere opmærksomhed. Social Engineering er defineret ved handlinger, der påvirker en person til at foretage sig noget, der ikke nødvendigvis er i den pågældendes egen interesse.

Det kan for eksempel være at skaffe sig adgang og informationer, der kan misbruges. Hertil kommer, at følgende angrebsmodus er vokset: CEO-fraud (hvor medarbejdere bliver narret til at overføre penge eller give adgang til systemer i den tro, at de agerer på en ordre fra ledelsen), Credential theft (legitimationsoplysninger, der bliver stjålet) og ransomwareangreb.

I henhold til ovenstående analyse bør private industrivirksomheder forholde sig til, hvordan de effektivt forebygger og bredt sikrer sig imod industrispionage og bevidst tager stilling til, hvad der er kritisk information for den enkelte virksomhed. Virksomhederne skal forholde sig til, hvem der har adgang til hvilke informationer i virksomheden, hvor informationerne er tilgængelige, og hvem og hvad der er en trussel mod virksomheden. Danske

industrivirksomheder kan blive meget bedre til systematisk at indsamle efterretninger om det aktuelle trusselsbillede mod netop deres virksomhed, ligesom de kan blive bedre til at kommunikere dette til deres ansatte og dermed bygge en stærkere sikkerhedskultur i virksomheden. Her er cybersikkerhed et af flere nødvendige nedslagspunkter, men det er også nødvendigt at forholde sig til den menneskelige faktor.

b. Gennemgang og revision af spørgsmål, værdisætninger og sammenhænge

Der er blevet tilføjet syv nye spørgsmål til SpionageTesten, ligesom en række spørgsmål er blevet opdateret/revideret i henhold til det gældende trusselsbillede. Afdækning af virksomhedens produktionsområde er opsat i alfabetisk rækkefølge for at gøre det lettere for brugeren at placere sin egen virksomhed. Spørgsmål omkring IT-sikkerhed er rykket frem i testen for at understrege vigtigheden af at beskytte sig mod IT-baserede angreb. Det er dog fortsat CERTAs vurdering, at governance og kultur er mindst ligeså afgørende elementer, når det kommer til at sikre sin virksomhed mest hensigtsmæssigt, så dette er fastholdt som testens første tematiske områder, inden IT-sikkerhed bliver adresseret.

De nye spørgsmål har blandt andet fokus på forebyggelse af social engineering og phishing-angreb. Det er her afgørende, at virksomhederne f.eks. har regler og procedurer for, hvornår og på hvilket grundlag betaling af regninger og overførsler kan finde sted.

Der er også tilføjet spørgsmål omkring kryptering af adgangskort samt registrering af den enkelte medarbejders fysiske adgang til virksomheden. Både præventivt og i forbindelse med konkrete efterforskninger kan det være hensigtsmæssigt at kunne spore den enkelte medarbejders adfærd.
Hertil kommer, at "almindelige" adgangskort ganske let kan kopieres, hvorfor en kryptering er hensigtsmæssig.

Der er også tilføjet spørgsmål, der skal få brugeren af testen til at overveje, hvilke anvendelsesmuligheder af virksomhedens IT (f.eks. tilkobling af private enheder på virksomhedens netværk samt tilkobling af virksomhedens enheder til private netværk) medarbejderen har.
Slutteligt er der indarbejdet et spørgsmål omkring indsamling og monitorering af den data, som medarbejderen genererer online. Dette hænger sammen med persondataforordningen og gældende regler omkring indsamling af data og overvågning af medarbejderne.

c. Opdatering af links og materialesamling

Der er udarbejdet en oversigt over nye materialer, som ligger til grund for den opdatering, der har været på selve siden:
https://spionagetesten.dk/links. Flere links er blevet opdateret med de nyeste udgaver, enkelte er udgået, og der er kommet nye tilføjelser. Mest interessant er måske PET's Projekt Insider, der sætter fokus på, hvordan medarbejdere enten med overlæg videregiver informationer eller utilsigtet udleverer erhvervskritisk information. Hertil kommer, at Center For Cybersikkerhed de senere år har publiceret flere specialiserede materialer. Der er fortsat fokus på at henvise til materialer på dansk, som ikke har et kommercielt sigte.

Effekt

Målet for SpionageTesten i 2016 var, at mindst 200 danske virksomheder skulle besøge hjemmesiden, og 100 virksomheder skulle gennemføre testen. I dag har der været mere end 180 gennemførte tests. De indkomne evalueringer viser en generel tilfredshed med værktøjet, og brugerne fremhæver, at testen bidrager til afdækning af sikkerhedsproblemer samt giver relevante anbefalinger, som er forståelige og anvendelsesorienterede.

Af data baseret på de anonyme besvarelser i SpionageTesten kan vi se, at:

- 50% af virksomhederne ikke har afdækket, hvad der er kritisk information for dem – altså, hvad de skal beskytte mod spionage
- Over 60% ikke har forholdt sig til industrispionage i forbindelse med rejser til udlandet
- 50% af virksomhederne ikke arbejder proaktivt med at skabe opmærksomhed om trusler internt i virksomheden

Dette er ganske alarmerende set i lyset af, hvor reel truslen er, og at f.eks. cyberkriminalitet ellers i høj grad optager danske virksomheder. I en undersøgelse, som Beredskabsstyrelsen og Dansk Industri udarbejdede i 2017, svarer 29% af de adspurgte virksomheder, at de inden for de sidste to år har stået i en krise på grund af cyberkriminalitet, og at dette vejer tungt i virksomhedernes bevidsthed. I samme undersøgelse peger 66% af de adspurgte virksomheder således på cyberkriminalitet som den største trussel.

Ønsket er, at endnu flere små og mellemstore industrivirksomheder ved at tage testen dels bliver opmærksomme på deres egne sårbarheder og dels bliver bevidste om, hvor de selv kan sætte ind for at øge sikkerheden.

Det er ikke muligt for nuværende at vurdere effekten af relanceringen. Erfaringerne fra den første lancering af SpionageTesten er imidlertid, at omfattende annoncering også fører til flere besøg og gennemførte tests. Det er muligt at gå tilbage til testen efter relanceringens forløb – projektaftalen er på seks måneders hosting af siden – og evaluere på de data, som testen har genereret.

Forankring og Formidling

Finansiering af selve domænet SpionageTesten.dk løber frem til og med udgangen af februar 2019. Det er i perioden fra lanceringen og seks måneder frem, at der er en forventning om, at virksomhedsledere fra små og mellemstore industrivirksomheder vil besøge og gennemføre testen.

Der er udarbejdet udkast til pressemeddelelse samt annoncematerialer til online annoncering. Forventet lancering er slut august 2018. Hertil kommer, at indsamlede materialer – analyser, værktøjer og andre tests – samt andre relevante nyheder om området løbende vil blive formidlet via SpionageTesten på Facebook.

PROJEKTNAVN:
SpionageTesten 2.0

BEVILINGSMODTAGER:
CERTA

PROJEKTANSVARLIG:
Jakob Dreyer

MAIL:
jd@certaintelligence.com

TELEFONNUMMER:
24 95 42 90

INDUSTRIENS FOND
FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation