Auteurs:
Ton Slewe en Peter Seelen

Fysieke en digitale beveiliging: niet langer aparte werelden!

Hoe kunnen organisaties zich beschermen tegen gecombineerde fysieke en digitale aanvallen?

Highlights

- Fysieke en digitale beveiliging zijn van oudsher gescheiden.
- Criminelen voeren gecombineerde aanvallen uit op fysieke en digitale beveiliging of kiezen de zwakste schakel in één van deze twee.
- Digitale beveiliging krijgt niet de aandacht die het verdient.
- Het samenbrengen van fysieke en digitale beveiliging onder leiding van een Chief Security Officer (CSO) leidt tot kostenverlaging en een betere bescherming.
- Door de CSO direct onder het hoogste management te brengen, krijgt de beveiligingsorganisatie slagkracht en het juiste management-commitment.

Stel je voor dat een medewerker van een IT-leverancier regulier onderhoud komt doen. Op het eerste gezicht niets vreemds. Later blijkt deze 'medewerker' in werkelijkheid een crimineel, die op vernuftige wijze het vertrouwen heeft misbruikt om aanpassingen te doen in de IT-infrastructuur van de organisatie. De crimineel kan door deze aanpassingen later van buitenaf ongeautoriseerd toegang krijgen tot IT-systemen.

Dit is precies wat er in 2013 gebeurde toen criminelen bij een Britse bank malafide IT-apparatuur installeerden[1]. Later gebruikten zij deze apparatuur om op afstand 1,5 miljoen euro te stelen . Bij deze 'bankoverval' werd er eerst fysiek toegang verschaft, waarna het ook mogelijk werd om toegang te krijgen tot banksystemen. Een combinatie van fysieke en digitale beveiligingsincidenten komen vaker voor. Zo waren het begin april 2018 enkele Russische inlichtingenofficieren die hun pijlen hadden gericht op de Organisatie voor het Verbod op Chemische Wapens (OPCW) in Den Haag[2]. Hiervoor benaderden zij het OPCW fysiek, om vervolgens te proberen het WiFi-netwerk van het OPCW te hacken. Organisaties moeten een meer innovatieve aanpak kiezen om zich beter te beschermen tegen dergelijke gecombineerde fysieke en digitale aanvallen. Hoe kunnen organisaties dat het beste doen?

Ontwikkelingen en dreigingen

Er zijn diverse ontwikkelingen gaande die relevant zijn voor fysieke en digitale beveiliging. Zo is er een toename van dreigingen, is er een steeds grotere afhankelijkheid van IT en groeit het besef tot de noodzaak van het integreren van deze nu nog vaak gescheiden twee werelden.

Groeiende afhankelijkheid van IT

We worden steeds afhankelijker van IT. Dat betekent dat het steeds belangrijker wordt om informatie goed te beveiligen. Daar komt bij, dat we steeds grotere hoeveelheden informatie genereren en communiceren. De ontwikkeling van mobiele netwerken, sociale media, hoge kwaliteit videobeelden en het snelgroeiende aantal aan het internet verbonden apparatuur spelen daar een belangrijke rol in. Het samenvoegen van verschillende soorten informatie zoals data, video en spraak heeft ertoe geleid dat deze informatie over hetzelfde netwerk wordt getransporteerd. Tevens wordt informatie door veel verschillende apparatuur gebruikt en wordt informatie steeds meer buiten de grenzen van organisaties opgeslagen.

Technologische ontwikkelingen voor aanval en verdediging

Op technologisch gebied zijn er verschillende ontwikkelingen. Fysiek is het bijvoorbeeld mogelijk om met drones spionage te plegen, apparatuur te stelen of zelfs mensen aan te vallen. Binnen de IT winnen innovatieve technologieën als kunstmatige intelligentie en machine learning (ML) snel terrein. Criminelen kunnen deze nieuwe technologieën gebruiken als aanvalsmiddelen. Organisaties kunnen ze daarentegen gebruiken om zichzelf te beschermen. Ook kunnen aanvallers middelen misbruiken die bedoeld zijn als verdediging. Het overnemen van een beveiligingscamera door een aanvaller is hier een voorbeeld van[3].

Onvoldoende aandacht voor integratie fysieke en digitale beveiliging

Traditioneel heeft bij beveiliging de focus meestal op fysieke of digitale beveiliging gelegen. Zo heeft de beveiliging van belangrijke personen veel meer aandacht gekregen van fysieke beveiliging en veel minder van digitale beveiliging. Bij digitale apparatuur is er een gebrek aan fysieke monitoring om het manipuleren ervan te kunnen detecteren. Het besef begint steeds meer te komen dat beide dreigingen en de combinatie ervan aandacht moeten hebben.

Groeiende dreiging vanuit statelijke actoren

Dreigingen vanuit statelijke actoren worden steeds meer zichtbaar en vormen de grootste digitale dreiging[4]. Zo gaf de AIVD aan de FBI cruciale informatie over de inmenging van Rusland in de Amerikaanse verkiezingen[5]. En statelijke actoren gebruiken soms criminele organisaties waardoor de grens hiertussen aan het vervagen is, met als gevolg dat het steeds moeilijker is om de daadwerkelijke opdrachtgever te achterhalen.

Uitdagingen bij het integreren van fysieke en digitale beveiliging

Om te bepalen hoe organisaties zich tegen gecombineerde fysieke en digitale aanvallen kunnen beschermen, moet er te worden gekeken naar de uitdagingen die organisaties op dit gebied hebben. Verschillende zaken spelen een rol in de scheiding tussen fysieke en digitale beveiliging.

Gedeelde of impliciete verantwoordelijkheid is geen verantwoordelijkheid

Een eerste uitdaging is van organisatorische aard. Beveiliging is vaak op diverse plekken in een organisatie belegd. De beveiliging van informatiesystemen en infrastructuur ligt meestal bij de IT-afdeling. De fysieke beveiliging is de verantwoordelijkheid van facilitaire zaken en is vaak uitbesteed aan een derde partij. Daarnaast zijn er soms aparte afdelingen voor informatiebeveiliging, die onderdeel zijn van de business- of risicomanagement. Het ontbreken van eindverantwoordelijkheid leidt ertoe dat er geen gedeeld management van incidenten over deze deelgebieden heen is. Hierdoor worden beveiligingsincidenten gemist, die anders wel waren opgemerkt. Er is dan ook geen eenduidige zicht op beveiligingsrisico's en -incidenten.

Onvoldoende commitment van hoogste management

Voor digitale beveiliging blijkt dat nog geen 25% van de Chief Information Security Officers (CISO's) direct aan het hoger management rapporteert[6]. In het geval van fysieke beveiliging is de afstand tot het hoger management nog groter. Vaak is de CISO onderdeel van de IT-afdeling en wordt beveiliging vanuit een IT-perspectief benaderd. Hierdoor kan er niet goed gestuurd worden vanuit de business op de juiste prioriteiten. Er is vaak onvoldoende budget beschikbaar om door beveiliging prangende bedrijfsissues op te lossen. Hierdoor staat het imago van het bedrijf op het spel en door de komst van nieuwe wetgeving wordt de kans groter dat boetes opgelegd worden. Beveiliging moet dan ook expliciet aandacht krijgen van het hoogste management.

Verschillende bronnen van identiteiten

Het ontbreken van de integratie tussen fysieke en digitale beveiliging is onder meer een gevolg van het organisatorisch apart beleggen daarvan. Een uitdaging die daarmee gepaard gaat is het hebben van meerdere bronnen met identiteitsgegevens. Deze identiteiten zijn cruciaal om een persoon of systeem te identificeren en te kunnen bepalen of die identiteit toegang tot bijvoorbeeld informatie heeft. Wanneer elk organisatiedeel haar eigen identiteiten beheerd, leidt dit tot inefficiënties. Het beheer van één identiteit moet immers tweemaal gedaan worden.

Ook kunnen identiteitssystemen over verschillende data beschikken. Volgens het ene systeem zou iemand nog toegang moeten hebben, terwijl het andere systeem aangeeft dat een medewerker al uit dienst is. Daar waar binnen organisaties wel integratie plaatsvindt van identiteiten voor toegang tot systemen en fysieke toegang, is dit veelal beperkt tot een integratie voor de eigen medewerkers. Voor gasten en externe partijen is er dan vaak nog een apart informatiesysteem. Het hebben van verschillende bronnen met identiteiten is inefficiënt en resulteert in beveiligingsrisico's.

Hoe worden fysieke en digitale beveiliging geïntegreerd? En wat levert het op?

Er kunnen diverse voordelen worden behaald met het integreren van digitale en fysieke beveiliging. Deze voordelen ondersteunen een positieve businesscase, waarmee investeringen kunnen worden verantwoord. Een holistische integratie van digitale en fysieke beveiliging zorgt voor een verbetering van de beveiliging en een verlaging van beveiligingsrisico's. De verlaging van deze risico's is op verschillende aspecten te realiseren, zoals organisatie, processen en technologie.

Stuur beveiliging centraal aan met commitment van het hoogste management

De scheiding van fysieke en digitale beveiliging voorkomt in belangrijke mate de samenwerking. Een eerste stap is om de organisatieonderdelen van fysieke en digitale beveiliging bij elkaar te brengen. Dit dient te gebeuren onder leiding van een Chief Security Officer (CSO), zodat er beter kan worden samengewerkt. Door de CSO net onder het hoogste management te plaatsen, krijgen fysieke en digitale beveiliging het juiste commitment en de benodigde middelen. Dit geeft de CSO de benodigde slagkracht om daadwerkelijk integratie te realiseren.

Deel beveiligingsinformatie en werk beter samen

Als de informatie van fysieke en digitale beveiliging wordt samengebracht, wordt het makkelijker om op basis van deze informatie samen te werken. Het samenbrengen van gegevens kan worden gedaan op basis van een geüniformeerd gegevensmodel, zoals STIX[7]. Hierdoor wordt het ook makkelijker om goede beveiligingsinformatie met andere partijen te delen en te ontvangen. Een organisatie is hiermee eerder voorbereid op nieuwe aanvallen. Dat stelt organisaties in staat om tijdig maatregelen te treffen. In Nederland speelt het NCSC[8] een belangrijke rol om dit soort informatie tussen partijen te delen.

Correleer beveiligingsinformatie en integreer incidentmanagement

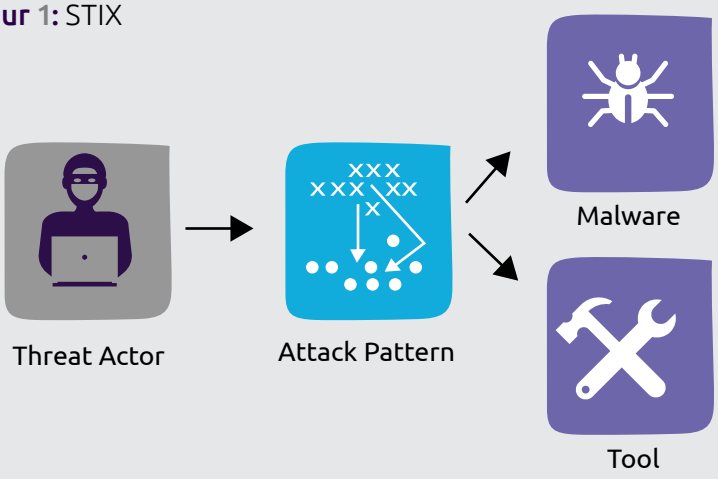
Als de beveiligingsinformatie in een gezamenlijk model wordt ondergebracht, wordt het veel makkelijker om informatie te correleren. Bij geïntegreerd incidentmanagement kan gebruik worden gemaakt van kunstmatige intelligentie om verbanden tussen fysieke en digitale gebeurtenissen te vinden en tijdig te reageren.

In het geval bescherming niet afdoende is, is het belangrijk dat er een adequate respons plaatsvindt. Dit betreft een respons op de detectie van een (potentieel) beveiligingsincident. Zo zou in het geval van een fysieke inbraak, preventief gegevens en/of cryptografische sleutels kunnen worden gewist van systemen wanneer deze dreigen te worden meegenomen.

Combineer fysieke en digitale beveiligingsmaatregelen

Op het gebied van bescherming en detectie kunnen gecombineerde maatregelen worden genomen. Zo is het mogelijk om voor informatiesystemen alleen toegang te geven, wanneer iemand fysiek aanwezig is. De fysieke aanwezigheid kan worden gerealiseerd door het scannen van een pas of door gezichtsherkenning. Een andere vorm van detectie kan plaatsvinden bij ongeautoriseerde toegang tot een draadloos netwerk. Er kan dan een camera worden ingeschakeld en op een potentiële dader worden gericht. Dit vergroot de mogelijkheden om aanvallen te voorkomen en te detecteren.

Figuur 1: STIX



Met STIX (Structured Threat Information Expression) is het mogelijk om informatie over dreigingen op een gestandaardiseerde manier uit te wisselen. In dit STIX voorbeelddiagram is er een dreigingsactor (threat actor) die een aanvalspatroon (attack pattern) gebruikt, dat bestaat uit een digitale (malware) en fysieke component (tool). Bij dit diagram wordt een geüniformeerd gegevensmodel gebruikt, dat systemen kunnen gebruiken om dreigingsinformatie.

Breng identiteiten samen

Goed identiteitsbeheer is een belangrijke voorwaarde voor een goede beveiliging. Zonder goed te weten wie iemand is, kun je niet goed bepalen wat iemand mag. Door identiteiten centraal bij te houden, hier goed beheer op te doen en waar nodig te synchroniseren, wordt aan een belangrijke voorwaarde voldaan.

Het integreren van verschillende processen en uitfaseren van gescheiden identiteitssystemen resulteert in een kostenbesparing en effectievere operatie. Dit stelt bedrijven in staat om de percepties die leven rondom de informatiebeveiligingsfunctie, te realiseren: het gebruik van beveiliging als drijfveer voor competitief voordeel en maakt een effectievere en efficiëntere organisatie mogelijk[9].

Integreer fysieke en digitale beveiliging!

Wanneer de fysieke en digitale omgeving als twee aparte werelden worden beschouwd, lopen organisaties grote beveiligingsrisico's. Criminelen maken van deze twee werelden gebruik om geavanceerde aanvallen uit te voeren of kiezen de zwakste schakel in één van deze twee werelden om hun doel te bereiken. Deze dreiging zal in de toekomst alleen maar toenemen. Het is daarom voor organisaties van essentieel belang om een holistische beveiligingsaanpak te kiezen, waarbij de fysieke en digitale beveiliging worden geïntegreerd!

[1]https://www.cso.com.au/article/527083/gang_exploits_both_physical_system_security_during_bank_robbery
[2]https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw
https://www.theguardian.com/world/2018/oct/04/visual-guide-how-dutch-intelligence-thwarted-a-russian-hacking-operation
[3]https://www.telegraph.co.uk/technology/2018/09/17/cctv-vulnerability-could-allow-cyber-criminals-hack-video-surveillance/
[4]NCTV – Cybersecuritybeeld Nederland (CSBN) 2018, https://www.nctv.nl/actueel/nieuws/2018/digitale-dreiging-in-nederland-neemt-toe.aspx
[5]https://nos.nl/nieuwsuur/artikel/2213762-hackteam-aivd-gaf-fbi-cruciale-info-over-russische-inmenging-verkiezingen.html
[6]IDC – The Modern Connected CISO, https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2019/01/The-Modern-Connected-CISO-5.pdf
[7]Structured Threat Information Expression, https://oasis-open.github.io/cti-documentation/stix/intro.html
[8]Nationaal Cyber Security Centrum, https://www.ncsc.nl
[9]IDC – The Modern Connected CISO, https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2019/01/The-Modern-Connected-CISO-5.pdf

Over de auteurs

Ton Slewe MBA CISSP is principal consultant bij Capgemini. Hij richt zich op cybersecurityvraagstukken bij publieke en private organisaties.

ton.slewe@capgemini.com

Ir. Peter Seelen CISSP CCSP is managing consultant bij Capgemini. Hij helpt organisaties met het inrichten en verbeteren van hun beveiliging, waarbij hij zich focust op Identity & Access Management (IAM) en Cloud Security.

peter.seelen@capgemini.com