THEMA'S: CRISISBEHEERSING CYBERCRIME TECHNOLOGIE
RUBRIEK: ONDERZOEK & ANALYSE

WAT ORGANISATIES NÚ MOETEN DOEN VOOR CYBERWEERBAARHEID

Foto: Shutterstock

3 februari 2026

AUTEURS: RICK VAN DER KLEIJ , MICHAËL BERTELS

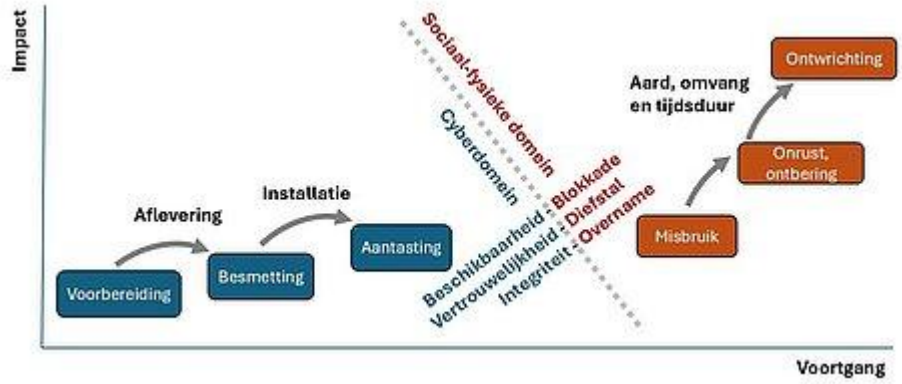
Cyberaanvallen beginnen digitaal, maar de gevolgen raken direct de samenleving. Het nieuwe cascademodel voor cyberweerbaarheid laat zien hoe verstoringen in IT kunnen uitgroeien tot maatschappelijke ontwrichting. Van phishing tot

fysieke impact: elke stap vraagt om samenwerking tussen cyberexperts en crisismanagers.

Cyber-aanvallen beginnen doorgaans in een technische IT-omgeving, waar cyber-specialisten deskundig zijn. Maar de gevolgen manifesteren zich in de echte wereld, waar crisismanagers de impact willen beheersen. Het model dat we hier presenteren, is een combinatie van de cyber kill chain, die werd ontwikkeld door Lockheed Martin om de stapsgewijze aanpak van een cyberaanval te beschrijven, en het cascademodel voor brand, ontwikkeld door het Nederlands Instituut Publieke Veiligheid om te beschrijven hoe de stapsgewijze uitbreiding van brand steeds meer impact heeft.

model slaat een
; tussen
rsecurity en
smanagement

Het model slaat een brug tussen cybersecurity en crisismanagement, waardoor het geschikt is voor samenwerking bij cyberweerbaarheid. De cascade verwijst naar een proces dat in stappen verloopt. Brand bijvoorbeeld, start in een voorwerp, ruimte of gebouw en neemt stapsgewijs toe. Net als de impact ervan. Hoe ziet dat eruit bij een cyberaanval?



VOORBEREIDING DOOR DE AANVALLER

Bij de eerste trede van de cascade, verzamelt de aanvaller informatie over het doelwit. Vervolgens ontwerpt hij een stuk gereedschap dat specifiek is gericht op een doelwit of doelgroep. De dader gaat bijvoorbeeld op zoek naar kwetsbaarheden in software dat in gebruik is bij hetbedrijf of ontwerpt een phishing-bericht. De impact is in dit stadium nog beperkt. Een maatregel die je kunt treffen in het sociaal-fysieke domein, om je te beschermen tegen de voorbereiding van een aanvaller, is geheimhouden van bedrijfsgegevens of actief opsporen van daders en hun financiers.

Escalatie naar de volgende cascadereactie, vindt plaats door het verzenden van het gereedschap naar het doelwit. Een maatregel die cybersecurityspecialisten kunnen nemen om zich te beschermen tegen deze escalatie, is bijvoorbeeld het blokkeren van afzenders en het installeren van software-updates die beschermen tegen zwakke plekken.

BESMETTING BIJ HET DOELWIT

In deze tweede cascadestap, is er bijvoorbeeld een phishing-bericht aanwezig in een mailbox van een slachtoffer of de aanvaller heeft al direct toegang via een kwetsbaarheid in de software. Bij deze stap is nog geen software geïnstalleerd. De beoogde slachtoffers worden blootgesteld aan ongewenste berichten. Een maatregel is een spamfilter op de mailserver.

Escalatie naar de volgende stap, vindt plaats door het installeren en activeren van ongewenste software of het benutten van een ongeoorloofde toegang. Een maatregel die beschermt tegen deze verergering, is het beperken van rechten van gebruikers om software te installeren en het scannen van systemen op verdachte software.

AANTASTING

Op dit punt in de cascade, is een of meer van de drie fundamentele prestaties van de IT-omgeving aangetast:

- Beschikbaarheid
- Vertrouwelijkheid
- Integriteit

Dit maakt een doelwit kwetsbaar voor misbruik. Een maatregel die hier op zijn plaats is, is het zelf uitschakelen van systemen om misbruik van data te voorkomen.

Escalatie naar het sociaal-fysieke domein, vindt plaats doordat de aanvaller gebruikmaakt van de aantasting. Op dit punt in het cascademodel, staan we op het grensvlak van waar het digitale domein overgaat naar de fysieke wereld. Dit is een belangrijke aanvulling op de reeds bestaande cyber kill chain.

s blijft de diefstal
anipulatie een
e onopgemerkt

Soms blijft de diefstal of manipulatie een tijdje onopgemerkt. De dader kan gegevens gebruiken om een volgende aanval voor te bereiden, of hij kan ongemerkt kwetsbaarheden introduceren, waar hij later gebruik van kan gaan maken. De aantasting breidt zich dan uit naar meerdere systemen of instanties.

IMPACT IN DE ECHTE WERELD

De impact in de fysieke omgeving is afhankelijk van de toedracht, aard, omvang en tijdsduur. Deze factoren zijn mede gebaseerd op het landelijk crisisplan digitaal van de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Dit plan biedt kaders voor effectief samenwerken tussen overheidsorganisaties, vitale aanbieders en niet-vitale sectoren. Laten we de factoren eens nader bekijken:

Toedracht: is er sprake van blokkade, diefstal of manipulatie? Door de beschikbaarheid aan te tasten, kan een dader een systeem blokkeren. Er is niets gestolen en gegevens zijn niet gemanipuleerd, maar een systeem reageert niet meer. Een maatregel kan zijn om uit te wijken naar een reservesysteem of een alternatieve werkwijze.
Bij het Monica ziekenhuis in Antwerpen en Deurne werden de digitale systemen getroffen door een gerichte cyberaanval, vermoedelijk met ransomware. Uit voorzorg werden alle servers uitgeschakeld, waardoor kritieke processen stilvielen: geplande operaties moesten worden afgeblazen, consultaties gebeurden tijdelijk met pen en papier en een deel van de patiënten werd overgebracht.

aders konden
vens bij de bron
veranderen

Wanneer de vertrouwelijkheid is aangetast, kunnen gegevens worden gestolen. Spionage, chantage en aantasting van de reputatie, kunnen daar gevolgen van zijn. Als maatregelen hiertegen, kun je zo min mogelijk informatie verzamelen (privacy by design), werken met aliassen (namen die niet te herleiden zijn naar echte personen) of informatie op een andere manier versleutelen. Zo werden er bij de hack van Clinical Diagnostics persoonlijke en testgegevens van bijna een half miljoen personen gestolen. Het bevolkingsonderzoek kon gewoon doorgaan, want systemen waren niet geblokkeerd. De testuitslagen zijn niet beïnvloed, want de daders konden gegevens bij de bron niet veranderen.

Door aantasting van de integriteit, kan een dader het systeem overnemen. Dat opent de deur naar stelen van geld en goederen en het ontregelen van fysiek verkeer. Fysieke beveiliging kan hier als maatregel dienen. Vorig voorjaar werd door een Russische hack een Noorse stuwdam opengezet, dankzij een zwak wachtwoord.

Aard van de getroffen instantie: om wat voor een instantie gaat het?
Een particulier bedrijf, hooguit met wat overlast of schade tot gevolg. Een gemeente of andere overheidsinstantie, waardoor dienstverlening aan burgers en bedrijven verstoord is. Hulpverleningsdiensten, die geen noodhulp meer kunnen leveren. Beheerders van infrastructuur, zodat weg- en waterverkeer stil komt te liggen, telecom uitvalt, geen drinkwater geleverd kan worden of de stroom uitvalt. Defensie, met militaire kwetsbaarheid als gevolg.

Omvang van de aanval: hoeveel systemen en instanties zijn betrokken?
Is slechts één systeem aangetast, dan kan de rest van het bedrijf blijven functioneren. Gaat het om een enkele instantie, dan is uitwijk naar een andere instantie mogelijk. Is een complete branche geraakt, kunnen bepaalde diensten of middelen helemaal niet meer beschikbaar zijn. Wanneer dat meerdere branches betreft, ontstaat er schaarste. En wanneer de schaal zo groot is dat we kunnen spreken van internationaal, dan kunnen buurlanden zelf niet helpen. Dat tast mogelijk zelfs de wil tot samenwerken in de EU of NATO aan.

Tijdsduur: hoelang gaat de verstoring duren?
Als dat maar kort is, dan kun je de verstoring even uitzitten. Maar wanneer het maar blijft aanhouden, dan worden burger, ondernemer en bestuurder -iedereen- geconfronteerd met schaarste.

VAN DIGITALE VERSTORING NAAR MAATSCHAPPELIJKE ONTWRICHTING

De combinatie van toedracht, aard, omvang en tijdsduur, bepaalt uiteindelijk de impact. Diefstal kan leiden tot schade en verontwaardiging, maar over het algemeen leidt het niet tot

fysieke effecten. Verontwaardiging kan enigszins beheerst worden door tijdige en eerlijke crisiscommunicatie. Daarbij is van belang om het slachtoffer centraal te zetten, de onvrede serieus te nemen en verantwoordelijkheid te nemen voor de gemaakte fouten. Niet ingrijpen door de overheid bij een grote hack, kan het vertrouwen in de overheid schaden.

kan al snel een
e impact
erkstelligen

Blokkades bij hulpverleningsdiensten en beheerders van infrastructuur, kunnen leiden tot chaos in de samenleving. Deze risico's zijn te beheersen, door terug te vallen op back-up systemen die onafhankelijk zijn van openbaar internet en op handbediening of pen en papier.

Door manipulatie van gegevens, kan een dader systemen opzettelijk verkeerd aansturen. Denk bijvoorbeeld aan alle bruggen openzetten of alle stoplichten op groen zetten. Dat kan al snel een grote impact bewerkstelligen. Deze risico's kunnen we beheersen door het inbouwen van een autorisatie door een mens, snelle herkenning en de mogelijkheid van het snel kunnen uitwijken naar handbediening. De combinatie van langdurige en omvangrijke schaarste, kan escaleren naar ontwrichting van de samenleving. Dat risico valt te beheersen met het inrichten van fysieke uitwijkmogelijkheden, zoals het noodpakket bij de burger thuis.

LEREN EN VERBETEREN

We kunnen cyberweerbaarheid vooral vergroten door lering te trekken uit cyberaanvallen. Het cascademodel helpt bij het kiezen van een leer- en verbeterstrategie. Ligt de focus op het succes en de bijdrage van één maatregel? Kies dan voor één afgebakende cascadestap of escalatie. Bijvoorbeeld:

- Waarom werd het phishing bericht niet herkend als spam en kwam het terecht in de mailbox van onze medewerkers?

- Hoe kunnen medewerkers leren deze berichten te herkennen en ze te melden?
- Hoe kunnen we phishing-websites blokkeren?
- Wat kunnen we doen met autorisatie zodat aanklikken van links niet leidt tot installatie?

Ligt de focus hoe verschillende maatregelen samenwerken? Neem dan meerdere cascadestadia en tussenliggende escalaties mee in de analyse. Bijvoorbeeld:

- Hoe kunnen we voorkomen dat diefstal van privacygevoelige gegevens leidt tot een grote publieke verontwaardiging?
- Hoe kunnen we voorkomen dat manipulatie van autorisatie in het toegangssysteem, leidt tot het openen van deuren in een penitentiaire inrichting?
- Is er een mogelijkheid om de snelwegkruizen handmatig te bedienen als het verkeersregelsysteem niet beschikbaar is?
- Welke rol speelt de verwachte impact in de fysieke wereld bij het besluit om eigen systemen af te sluiten?

Kortom, het cascademodel voor cyberweerbaarheid laat zien hoe cybersecurity en crisisbeheersing samengaan. Is de impact van cyberverstoring hoog, dan rechtvaardigt dat extra investering in cybersecurity. <<

Michaël Bertels werkt bij de veiligheidsregio Brabant-Noord als crisisteam ontwikkelaar. Rick van der Kleij is lector Cyberweerbare Organisaties bij Avans Hogeschool en cybersecurity onderzoeker bij TNO. Zij zijn bereikbaar voor vragen of discussies: m.bertels(at)vrbn.nl en r.vanderkleij1(at)avans.nl.

GERELATEERDE ARTIKELEN

‘CYBERCRIME PLEGEN IS GEMAKKELIJKER GEWORDEN’

Lees dit artikel

DE AANPAK VAN GEDIGITALISEERDE CRIMINALITEIT MOET BETER

Lees dit artikel

VEELBELOVENDE POLITIEPROJECTEN TEGEN CYBERCRIMINALITEIT

Lees dit artikel