



Feitencheck

# Het belang van snel herstel na cyberaanvallen



Terwijl de wereldwijde schade door cyberaanvallen in 2015 3 biljoen dollar bedroeg, zal dit cijfer in 2024 naar verwachting meer dan verdrievoudigd zijn<sup>1</sup>. Alleen al in Duitsland bereikte de schade door gegevensdiefstal, industriële spionage en sabotage een alarmerend record van 266 miljard euro<sup>2</sup>.

Vooraf losgeldaanvallen vullen steeds meer de portemonnee van cybercriminelen: Volgens een onderzoek van Bitkom (Duitse branchevereniging voor digitale economie) waren zes op de tien bedrijven tussen september 2023 en september 2024 het doelwit van een dergelijke aanval. Bijna een op de drie bedrijven in Duitsland (31%) leed schade in de vorm van productiestilstand, kosten voor IT-dienstverleners of betalingen aan de daders.

Slechts 40% van de getroffen bedrijven kon de gegevens zelf herstellen. De aanbeveling van Felix Kuhlenkamp, hoofd van het beveiligingsbeleid bij Bitkom e.V., komt dan ook niet als een verrassing: “Alle bedrijven moeten hun technische IT-beveiliging opvoeren, medewerkers trainen om **aanvallen in een vroeg stadium te herkennen en vooral regelmatig back-ups maken.**”



Maar back-ups alleen zijn niet genoeg.

Het is niet alleen cruciaal dat er een back-up is van de gegevens, maar ook dat de herstelstrategieën probleemloos werken in geval van nood. De snelheid van het herstelproces speelt ook een belangrijke rol, want elke vertraging vermenigvuldigt de economische schade die wordt veroorzaakt door downtime.

Feit

## Dit is hoe lang bedrijven nodig hebben voor het herstel

De tijd om volledig te herstellen van een cyberaanval duurt wereldwijd gemiddeld 7,3 maanden, waarbij 5% van de organisaties er meer dan 18 maanden over doet en 1% ervan uitgaat dat volledig herstel nooit plaatsvindt<sup>3</sup>.

Als we de gegevens van het wereldwijde onderzoek isoleren voor de DACH-regio alleen, is het beeld nog somberder: Gemiddeld duurt het hier 8,6 maanden voordat een volledig herstel optreedt, waarbij 7% er meer dan 18 maanden over doet en 2% ervan uitgaat dat een volledig herstel nooit zal plaatsvinden<sup>4</sup>.

Goed voorbereide organisaties herstellen echter 41% sneller van inbreuken op de beveiliging dan minder goed voorbereide organisaties. Het Cyber Recovery Readiness Report somt 5 criteria op die niet alleen de risico's maar ook de impact van beveiligingsinbreuken aanzienlijk verminderen:

**1****Systemen voor vroegtijdige waarschuwing**

Gebruik van beveiligingshulpmiddelen voor vroegtijdige detectie van cyberrisico's.

**2****Geïsoleerde locatie voor noodgevallen**

Voorziening van een afzonderlijke, veilige omgeving voor snel herstel van activiteiten na cyberaanvallen.

**3****Onwijzigbare gegevensback-up**

Het onderhouden van een geïsoleerde, fraudebestendige gegevensback-up in een externe infrastructuur.

**4****Gestructureerde respons**

Gedefinieerde noodplannen, rollen en processen voor een efficiënte reactie op

**5****Meetbare paraatheid**

Regelmatige herstel oefeningen en risicobeoordelingen om de effectiviteit van de plannen te testen en mogelijke zwakke punten te identificeren.

Feit

## Dit is hoeveel een beveiligingslek kost

De kosten van productiestilstand hangen grotendeels af van de duur en de grootte van het bedrijf. Een bedrijf met 100 werknemers, een productie van 70% en een gemiddeld uurloon van 35 euro heeft al te maken met stilstandkosten van  $100 \times 35 \times 0,7 = 2.450$  euro per uur.

Voor grote bedrijven kan dit al snel resulteren in schade die in de miljoenen loopt. Zelfs de sky is niet de limit - zoals gegevens van Delta Airlines bewijzen. Toen het datacenter van de luchtvaartmaatschappij 5 uur buiten werking was, bedroeg de schade al 150 miljoen dollar<sup>5</sup>.

En het was gewoon een stroomstoring, zonder de extra kosten die een beveiligingslek met zich meebrengt:

- IT-overuren voor herstel
- Externe cyberexperts voor forensisch onderzoek
- PR-budget voor crisiscommunicatie met werknemers, zakenpartners en het publiek<sup>7</sup>

## Verloren vertrouwen van klanten

De financiële gevolgen van cybercriminaliteit gaan echter veel verder dan de genoemde directe kosten. Bedrijven die het slachtoffer worden van inbreuken op de beveiliging krijgen vaak te maken met reputatieschade op lange termijn, een verminderd vertrouwen van klanten en hogere kosten voor klantenwerving: 65% van de consumenten zegt het vertrouwen in een bedrijf te verliezen na een datalek en 85% wil geen zaken meer doen met een bedrijf als ze zich zorgen maken over de beveiligingspraktijken<sup>6</sup>.

Hoewel de cijfers niets zeggen over de impact van hersteltijd op het vertrouwen van klanten, is één ding duidelijk: een snel herstel kan helpen om klanten gerust te stellen en is al een eerste stap in het terugwinnen van verloren vertrouwen.

## Dalende aandelenkoersen

Met het verlies aan vertrouwen van klanten en beleggers daalt ook de aandelenkoers. Volgens een analyse van Morningstar zakt de aandelenkoers met 2-3% binnen de eerste 4 dagen na de aankondiging. Hoewel enkele bedrijven zich al na 12 dagen herstellen, keldert de aandelenkoers in de meeste gevallen verder en bereikt gemiddeld na 59 dagen zijn laagste punt, met een waardeverlies van 5,3% ten opzichte van de sectorindex. Terwijl de sectorindices van de geanalyseerde bedrijven na een jaar gemiddeld 10,15% winst boekten, noteerden de bedrijven die het slachtoffer werden van een cyberaanval een waardeverlies van 0,65%.

Met de Data Privacy and Security (DP&S) Management Score heeft Morningstar nog een hulpmiddel voor risicobeoordeling. Hoewel de beleggingsexperts niet openlijk communiceren hoe dit precies wordt berekend, zou het niet te veel moeten verschillen van de MSCI-berekening. Deze omvat verschillende factoren die ook een indirecte invloed hebben op de herstelsnelheid en die sterk doen denken aan de vijf criteria die in het begin werden genoemd. Zo worden bijvoorbeeld de training van werknemers, verantwoordelijkheden en de reikwijdte en aard van het noodplan beoordeeld voor deze score.

Het verschil tussen bedrijven met een hoge DP&S Management Score en bedrijven met een lage score was significant: terwijl bedrijven met een score van 0 of helemaal geen score na één jaar gemiddeld 12,42 procentpunten achterliepen op hun sector, lagen bedrijven met een score van 75 of hoger bijna op gelijke hoogte met hun sector (-1,74<sup>8</sup>).

## Organisatorische uitdagingen

In de dagen na een cyberaanval bevinden getroffen bedrijven zich in een noodtoestand. Ze staan onder enorme druk om zo snel mogelijk weer online te zijn om de hierboven genoemde redenen. Paradoxaal genoeg kan een te snel herstel ertoe leiden dat reeds gecompromitteerde systemen opnieuw worden geactiveerd en de schade nog groter wordt. Om met de nodige expertise te kunnen reageren, is een koel hoofd en onder geen beding overhaaste expertise nodig, die steeds vaker ontbreekt in tijden van een tekort aan geschoold personeel.

Eind 2022 waarschuwde de BSI (Duitse federale autoriteit voor informatieveiligheid) voor een “fundamenteel tekort” aan personeel voor incidentrespons. Bijzonder ernstig: zelfs externe experts zijn “soms volledig bezet en zijn dan niet in staat om nieuwe incidenten te accepteren”.<sup>9</sup> Alleen al de zoektocht naar expertise dreigt het bedrijf tot stilstand te brengen.

Cyberherstel is een arbeidsintensief proces dat niet alleen de expertise van IT-specialisten vereist. Managers, de juridische afdeling, communicatieteams en soms zelfs wetshandhavinginstanties moeten er ook bij worden betrokken. Een duidelijke verdeling van rollen en verantwoordelijkheden is essentieel voor een succesvol herstel. Een effectief herstelplan moet duidelijk definiëren welke mensen verantwoordelijk zijn voor welke functies.



## Succesfactoren voor een snel herstel

“Ons onderzoek toont aan dat de bedrijven met de beste cyberweerbaarheid die bedrijven zijn die hun herstelstrategieën voortdurend testen en optimaliseren. Ze leren van elk beveiligingsincident en versterken hun verdediging”, zegt Commvault CTO Brian Brockway, verwijzend naar het bovengenoemde Cyber Recovery Readiness Report<sup>10</sup>. Er kan echter ook worden geleerd van de incidenten bij andere bedrijven.

### Praktijkvoorbeeld Maersk

4 miljoen containers, 1000 magazijnen, 900 schepen, 1 malware. De NotPetya-aanval, oorspronkelijk gericht op Oekraïne, maakte gebruik van een gecompromitteerde update van de Oekraïense besturingssoftware M.E.Doc in 2017 en infecteerde ook wereldwijd opererende bedrijven - waaronder Maersk. Nadat de malware toegang wist te krijgen tot de referenties van domeinbeheerders, verspreidde deze zich snel over het hele netwerk.

Om 10 uur 's ochtends merkte het netwerkbewakingsteam van Maersk de eerste onregelmatigheden op, voordat de verbinding met het wereldwijde netwerkbewakingscentrum in het Verenigd Koninkrijk kort daarna volledig wegviel. Het hele netwerk werd onmiddellijk uitgeschakeld, maar tegen die tijd waren 49.000 laptops en computers geïnfecteerd en 1200 bedrijfskritische applicaties ontoegankelijk geworden. De hele Active Directory bleek verloren, telefoonlijsten waren gesynchroniseerd en dus ook verdwenen. Maersk was zijn wereldwijde communicatiecapaciteit kwijt en had aanvankelijk geen duidelijkheid over de aard en omvang van de aanval.

De volgende ochtend was Microsoft erin geslaagd om één computer te ontsleutelen, maar dit kostte 22.000 uur rekenwerk en de code hielp alleen bij dit ene apparaat. Ontcijfering op grote schaal was daarom onmogelijk. Verloren gegevens proberen te herstellen was ook te riskant, omdat dit ook de malware opnieuw zou kunnen activeren. De enige optie was om helemaal opnieuw te beginnen.

Een gelukkig toeval kwam Maersk te hulp in de vorm van een stroomstoring in Lagos, Nigeria. Het kantoor daar was offline op het moment van de aanval en had een complete, niet-versleutelde kopie van de Active Directory, die de basis vormde voor het opnieuw opbouwen van het hele netwerk.

Na 14 dagen had Maersk de basis bedrijfstechnologie hersteld en was weer operationeel, zij het met een verminderd volume. Het duurde nog eens vier weken om de volledige capaciteit te bereiken, voornamelijk door de aanschaf van 17.000 nieuwe eindapparaten. In totaal veroorzaakte het incident voor 350 miljoen dollar schade.

## Lessons learnt

### Partnerschappen, transparantie en veerkracht

Maersk heeft cruciale lessen geleerd uit het incident, die zijn geïntegreerd in de bedrijfscultuur en de beveiligingsstrategie. De belangrijkste “geleerde lessen”, die ook essentieel zijn voor andere bedrijven, kunnen als volgt worden samengevat:



#### Partnerschappen zijn cruciaal

Maersk vertrouwde vanaf het begin op externe expertise. Deloitte werd gekozen als forensische partner, niet vanwege een langdurige evaluatie, maar vanwege de geografische nabijheid en de snelle beschikbaarheid van middelen. De ondersteuning van technologiepartners zoals IBM en Microsoft bij de wereldwijde distributie van gegevens was essentieel voor de snelle reconstructie.



#### Transparantie schept vertrouwen en steun

Maersk koos voor open communicatie, zowel intern als extern. Regelmatige video-updates hielden medewerkers en klanten op de hoogte. Externe transparantie speelde een belangrijke rol bij het verkrijgen van goodwill en zelfs concrete steun van andere bedrijven, bijvoorbeeld in de vorm van geleende Azure cloud experts.



#### Focus op herstelmogelijkheden

De mogelijkheid om kritieke infrastructuur zoals Active Directory, DHCP en DNS snel te herstellen is van vitaal belang om te overleven. Maersk had 14 dagen nodig om de basale bedrijfstechnologie te herstellen. Nu is alles erop gericht om al na 24 uur weer te kunnen functioneren.



#### Veerkracht door redundantie en back-up

De toevallige Lagos-back-up benadrukt het belang van redundante systemen en up-to-date, offline back-ups van kritieke infrastructuurcomponenten zoals Active Directory.<sup>11</sup>

## Conclusie

De beschikbare gegevens laten een aanzienlijke toename zien van economische verliezen als gevolg van cybercriminaliteit, zowel wereldwijd als in Europa. Het schadebedrag is in slechts een paar jaar tijd meer dan verdrievoudigd en vooral ransomware-aanvallen vormen een groeiende bedreiging voor bedrijven.

Een belangrijk probleemgebied is de tijd die bedrijven nodig hebben om volledig te herstellen van cyberaanvallen. Het wereldwijde gemiddelde is meer dan zeven maanden, en zelfs langer in de Duitstalige (DACH-) regio. Deze lange downtime leidt tot aanzienlijke kosten door productieverlies, IT-herstelmaatregelen en reputatieschade.



## Referenties

- 1 <https://cybersecurityventures.com/cybersecurity-almanac-2024/>
- 2 <https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/>
- 3 <https://learn.fastly.com/rs/025-XKO-469/images/Global%20Report%202024%20-%20Global%20Deck.pdf?version=0>
- 4 <https://learn.fastly.com/rs/025-XKO-469/images/DACH%20%20Deck%20-%20Global%20Report%202024%20.pdf?version=0>
- 5 <https://www.five9sdigital.com/knowledge/delta-airlines-our-5-hour-data-center-outage-cost-us-usd150m/>
- 6 <https://www.kiteworks.com/de/cybersecurity-risikomanagement/anstieg-von-cyberangriffen-um-92-in-zwei-jahren-der-risiko-score-index-2024-enthuehlt-alarmierende-trends/>
- 7 <https://www.techbold.at/blog/die-ransomware-rechnung-was-ein-hackerangriff-in-summe-kostet>
- 8 <https://www.sustainalytics.com/esg-research/resource/investors-esg-blog/analysis-strong-data-privacy-and-security-management-pays-off>
- 9 <https://www.handelsblatt.com/technik/it-internet/it-sicherheit-an-der-belastungsgrenze-experten-fuer-die-cyberabwehr-werden-knapp/28881154.html>
- 10 <https://ap-verlag.de/cyberresilienz-und-cyber-recovery-vorbereitung-zahlt-sich-aus/90581/>
- 11 <https://www.csoonline.com/article/567845/rebuilding-after-notpetya-how-maersk-moved-forward.html>



**FAST LTA**  
Rüdesheimer Str. 11  
80686 München  
info@fast-lta.de  
**www.fast-lta.de**

Design,  
Entwicklung  
und Support  
in **Deutschland**

