CHUBB®

Baanbrekend in risico's voor de ICT-sector

Bewustwording van Cyberrisico's voor IT-bedrijven

CHUBB®

Bewustwording van Cyberrisico's voor IT-bedrijven

Auteurs

Barry Schütte
Manager Industry Practices Benelux, Chubb

Wouter Wissink
Senior Principal Cyber Risk Engineer & Technology Industry Practitioner, Chubb

Cyberbeveiliging is een risicogebied dat bijzondere aandacht vereist, vooral nu de kosten van cybercriminaliteit tegen 2025 naar verwachting zullen stijgen tot 10,5 biljoen dollar, volgens Cybersecurity Ventures. Vooral IT-bedrijven zijn kwetsbaar voor hackers, want als tussenpersonen vormen ze een doelwit om malware of ransomware in één klap te distribueren naar meerdere bedrijven.

De aanvallen op Kaseya en SolarWinds zijn twee bekende voorbeelden van de schade die kan worden veroorzaakt door steeds geavanceerdere criminelen. Georganiseerde hackers zijn steeds meer geïnteresseerd in het te gelde maken van hun activiteiten en daarom is ransomware nu het grootste cybergevaar, volgens het Europese Agentschap voor Cyberbeveiliging.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Om cybercriminaliteit een halt toe te roepen, is een robuuste beveiliging en continue aandacht voor beveiligingsmaatregelen nodig. Risico's kunnen significant worden beperkt door bepaalde cyberhygiënemaatregelen in acht te nemen. Maar wat kunnen IT-bedrijven doen om zichzelf te beschermen, nu cyberaanvallen steeds doelgerichter en geavanceerder worden?

Veel voorkomende risico's

Die bedrijven hebben te maken met twee fundamentele risico's die nauw met elkaar verbonden zijn, namelijk aanvallen op hun eigen omgevingen en aanvallen die hun klanten schade toebrengen. Een cyberaanval op een softwareontwikkelaar of -distributeur kan leiden tot diefstal van vertrouwelijke gegevens, die vervolgens kunnen worden misbruikt door hackers om directe toegang te krijgen tot een klantenomgeving. Als een IT-bedrijf wordt aangevallen door ransomware, is het mogelijk niet meer in staat dienstverlening aan zijn klanten te bieden. Of software die is aangetast door backdoor-malware kan ongewild worden verkocht aan klanten, wat de deur opent voor een aanval op honderden of duizenden bedrijven.

Cybercriminelen kunnen ook schade aanrichten door toegang te verkrijgen tot klanten via Managed Service Providers (MSP's), waarschuwt Wouter Wissink, Senior Principal Cyber Risk Engineer & Technology Industry Practitioner bij Chubb.

De zakelijke, financiële en imagogerelateerde gevolgen voor IT-bedrijven kunnen enorm zijn, aldus Barry Schütte, Industry Practices Manager bij Chubb. "Bezorgde klanten kunnen bijvoorbeeld overstappen naar een concurrent, en dat heeft een impact op de winst", licht hij toe.

Moeilijke bedrijfsbeslissingen

Welke lessen kunnen we trekken uit de aanvallen op Kaseya en SolarWinds? In het geval van de Amerikaanse multinational Kaseya werden in juli 2021 kwetsbare punten in de VSA-software (Virtual System Administrator) - geleverd aan MSP's en IT-teams - door hackers uitgebuit in een zero-day-aanval.

Cyberhygiëne best practices checklist

- Kunt u de risico's identificeren waarmee uw bedrijf en klanten worden geconfronteerd?
- Weet u wat u moet doen om blootstelling aan die risico's te voorkomen?
- Zijn er maatregelen ingevoerd om cyberrisico's te detecteren?
- Bestaat er een duidelijk plan voor hoe te reageren als u wordt gehackt?

"Als de 'tussenpersoon' lopen MSP's juist meer cyberrisico's"

https://www.rapid7.com/products/insightvm/vulnerability-report-hub-page/

"Die tussenperiode valt heel moeilijk te beschermen," aldus Wissink. "Softwarebedrijven hebben minstens een week nodig om dit soort problemen op te lossen en ondertussen blijven de softwareontwikkelaars blootgesteld aan risico."

Het verlies van Kaseya was beperkt tot ongeveer 50 klanten, maar wereldwijd tot wel 1.500 andere bedrijven verder in de bedrijfskolom zouden ook door ransomware zijn getroffen.

De blootstelling aan dergelijke aanvallen stijgt snel. In 2021 verdubbelde het aantal zero-day-aanvallen, volgens een onderzoek van Rapid7. "Dit is het meest kritieke risicogebied, want het is heel moeilijk te beheren," aldus Wissink. Hij raadt getroffen bedrijven aan om nog dezelfde dag aan klanten te melden dat een systeem gehackt is, snel de systemen offline te zetten en de klanten op de hoogte te houden.

"Dat kan voor sommige bedrijven erg moeilijk zijn," waarschuwt hij. "Je zegt eigenlijk tegen je klanten dat je bedrijfsmodel niet meer veilig is en dat ze offline moeten gaan."

Achterdeurtactieken

Zes maanden voor de aanval op Kaseya vond het zogenaamde "Solarigate-incident" plaats, een hackersaanval waarbij de cybercriminelen malware toevoegden aan updates in het Orion-softwaresysteem van SolarWinds, een systeem dat veelvuldig wordt gebruikt door bedrijven die IT-resources beheren.

"De hackers konden zich toegang verschaffen tot de ontwikkelomgeving", zegt Wissink. De malware verspreidde zich ongemerkt als onderdeel van een standaard software-update voor klanten en zorgde zo voor een achterdeur naar hun IT-systemen. Ongeveer 18.000 klanten werden getroffen, waaronder ook Amerikaanse overheidsinstellingen en internationale merken. Volgens Wissink "hadden de juiste cyberpreventiemaatregelen die aanval kunnen voorkomen."

Nieuwe trends

Welke trends zien verzekeraars momenteel? Bedrijven verbeteren hun eigen beveiligingsniveaus, zegt Schütte, zodat cybercriminelen hun pijlen steeds meer richten op toeleveranciers. Als 'tussenpersoon' worden MSP's geconfronteerd met grote cyberrisico's en de groei van deze markt gaat gepaard met een stijging in het aantal claims.

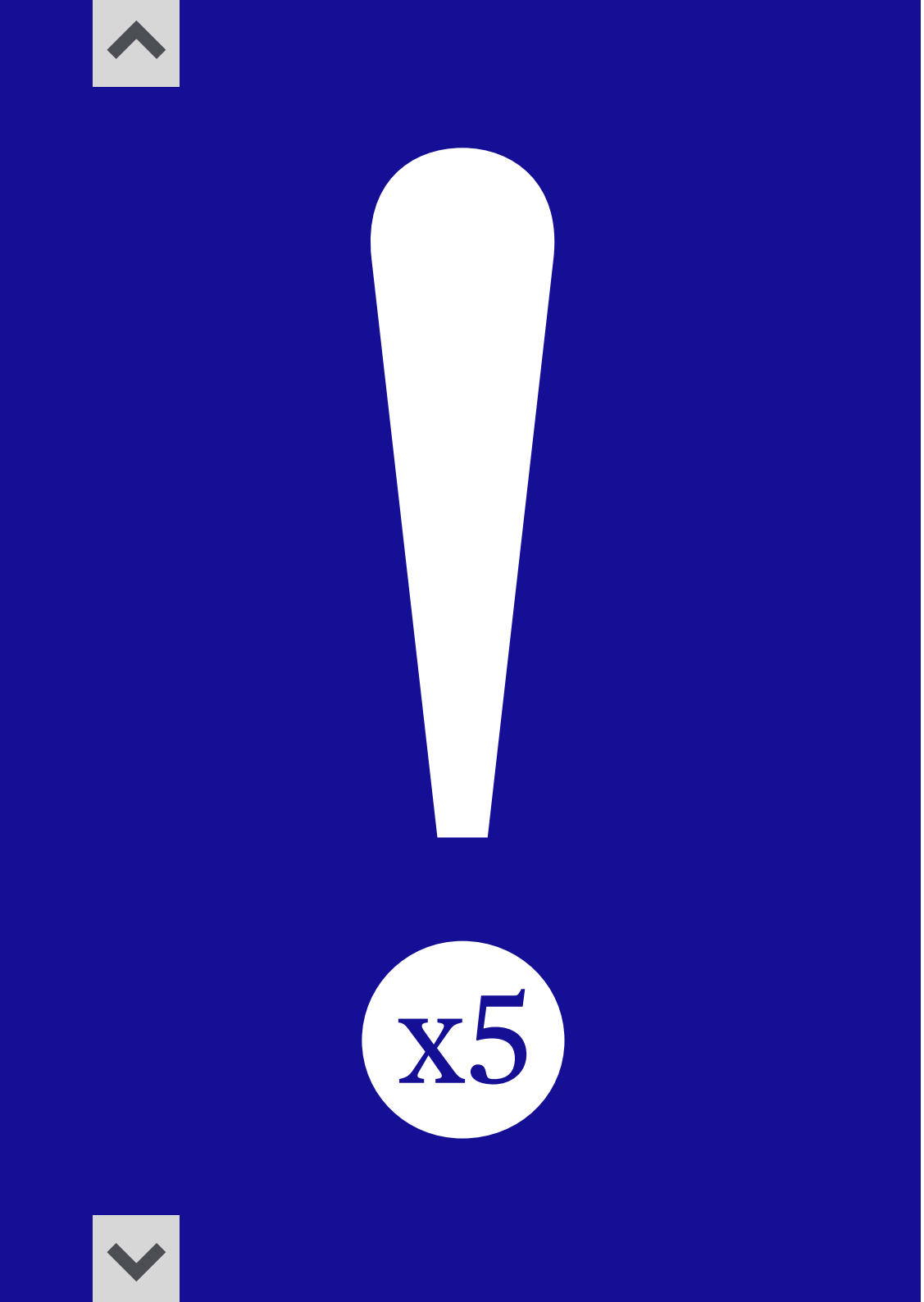
"Platform as a Service (PaaS) en Software as a Service (SaaS) zijn ook meer blootgesteld aan risico's," voegt hij toe. "Het risicoprofiel is dus aanzienlijk gestegen met deze verschuiving van lokale softwaresystemen naar platform- of cloudgebaseerde bedrijfsmodellen."

Zorgplicht is een ander opkomend risicogebied. In de relatie tussen een leverancier en klant wordt een IT-bedrijf meestal beschouwd als de expert, legt Schütte uit. "De verantwoordelijkheden van het bedrijf gaan meestal verder dan wat in een overeenkomst is geschreven, wat betekent dat de aansprakelijkheidsrisico's toenemen." Een aanbieder raadde een klant aan om extra beveiligingsmaatregelen te nemen, maar zette dit advies niet op papier. Toen de klant later het slachtoffer werd van een ransomware-aanval en het IT-bedrijf voor de rechter daagde, werd het IT-bedrijf aansprakelijk bevonden.

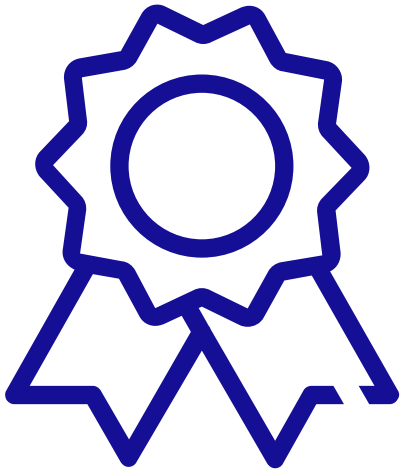
Dus hoe kunnen deze risico's worden opgevangen via goede cyberhygiëne? We onderzoeken de beste praktijken voor IT-bedrijven op basis van vier stappen: identificeren, voorkomen, detecteren en reageren.

De risico's bepalen

Het vaststellen van cyberrisico's is gewoon een kwestie van robuust risicobeheer, volgens Wissink en Schütte. IT-bedrijven moeten exact identificeren welke producten en diensten ze leveren om in te schatten welke risico's ze lopen. Maken ze software? Distribueren ze software? Zijn ze een MSP? Slaan ze wachtwoorden voor klanten op?



"In plaats van één groot risico zien we vandaag de dag vijf grote, dus het risico voor IT-bedrijven is vijf keer zo hoog als 10 tot 15 jaar geleden"



Met een Information Security Management System (ISMS) kunnen bedrijven deze zaken in kaart brengen. Dankzij een dergelijk centraal beheerd systeem kunnen ze hun praktijken op het vlak van databeveiliging beheren, monitoren en waar nodig herzien.

Hoewel softwareontwikkelaars over het algemeen "heel wat inspanningen" leveren om een veilig product op te leveren, zegt Wissink, vergeten ze vaak dezelfde beveiliging te garanderen voor hun eigen omgeving. Klanten worden bijvoorbeeld regelmatig gevraagd om software te downloaden van een website die niet goed beveiligd is.

Beschermen en versterken

Om cyberaanvallen te stoppen, zijn minstens standaard hygiënemaatregelen nodig, waaronder multifactor-authenticatie, adequate bewustwordingstraining van werknemers, firewalls, het scannen naar phishing-mails en het filteren van websites.

"Maar IT-bedrijven zouden juist de beste beveiligingsmaatregelen ingevoerd moeten hebben, gelet op de grotere potentiële impact van verliezen door een wijdverspreide gebeurtenis en de grotere verantwoordelijkheden op het gebied van zorgplicht," adviseert Wissink. Hij zegt dat bedrijven een PAM-systeem (Privileged Access Management) nodig hebben. De PAM-tool beschermt identiteiten, met speciale toegang of machtigingen die verder gaan dan die van gewone gebruikers. Dit is vooral belangrijk voor MSP's, waar veel werknemers toegang hebben tot meerdere programma's via een centraal softwarepakket.

Bedrijven in softwareontwikkeling moeten ook hun netwerk afschermen en beveiligen met extra tools waartoe alleen ontwikkelaars toegang hebben, benadrukt Wissink. "Die ontwikkelingsomgeving mag geen automatische verbinding hebben met de rest van het bedrijf."

Overige goede maatregelen om risico's te reduceren en de bedrijfscontinuïteit te helpen zijn het continu testen en offline opslaan van back-ups en een vlijmscherpe focus op de versleuteling van wachtwoorden en andere gegevens. Ook het aanstellen van een toegewijde IT-beveiligingsmanager is een slimme zet.

"Bedrijven moeten gegevens beschermen maar moeten ook een waterdichte overeenkomst met de klant sluiten over hoe hun gegevens op te slaan en te verwerken", zegt Schütte.

Maar bij preventie draait het niet alleen om technische voorzorgsmaatregelen. Het draait ook om communicatie en contractuele overeenkomsten over het serviceniveau en over gegevensbescherming. "Een IT-bedrijf, en vooral een MSP, heeft de zorgplicht om klanten te waarschuwen voor en in te lichten over mogelijke gebrekkige beveiligingsniveaus van een specifieke klantomgeving," voegt Wissink toe. "Klanten moeten schriftelijk worden ingelicht en dit moet ook worden gedocumenteerd, om zich te beschermen tegen aansprakelijkheid."

Volgens Schütte lopen veel IT-bedrijven achter wat betreft preventiemaatregelen om veilige software te ontwikkelen (security by design). Dit geldt ook voor penetratie- en kwetsbaarheidstesten, code review en opleiding in het schrijven van "veilige" code (de OWASP Top 10 kan helpen).

Softwareontwikkelaars die niet-kritische software ontwikkelen mogen de noodzakelijkheid van dergelijke regels niet negeren", adviseert hij.

"Vandaag de dag is elk bedrijf een doelwit voor hackers," waarschuwt Wissink.

Belangrijkste bevindingen

- **Aanvallen op MSP's zijn de belangrijkste** opkomende trends in claims
- **IT-bedrijven moeten beter beveiligd zijn** tegen zero-day-aanvallen
- **De risico's op het vlak van zorgplicht** nemen toe en zouden bij elk bedrijf op de radar moeten staan
- **Een ISMS (Information Security** Management System) kan helpen risico's te detecteren en beheren
- **Gebruik een PAM-tool (Privileged Access Management)** om hackers tegen te houden
- **Scherm uw softwaresysteem af van de rest** van het bedrijf
- **Communicatie met klanten is cruciaal voor** een goede cyberpreventie
- **Implementeer afdoende beleidsregels voor** beveiligde softwareontwikkeling
- **Een networkmonitoringsysteem** (24/7 opvolging) is een goed idee
- **Vergeet niet formele aanvallenrespons- en** calamiteitenplannen plannen op te stellen
- **Vergeet niet om back-ups continu te testen** en offline op te slaan

Cyberinbreuken detecteren

Opvolgings- en detectiesoftware zoals Endpoint Detection and Response (EDR) is een must voor IT-bedrijven, net als goede firewalls of een netwerkmonitoringsysteem, dat dag en nacht wordt opgevolgd door een intern of extern beveiligingscentrum. "Het is van cruciaal belang een hacker bijtijds op te merken zodra hij het systeem binnendringt," benadrukt Wissink.

Brandjes doven

Wissink en Schütte zijn het erover eens dat een van de belangrijkste bedrijfskritische elementen voor het bestrijden van cyberaanvallen een duidelijk incidentenresponsplan is. Met een tijdige planning kan een bedrijf gepast en snel reageren in geval van een aanval. Voor een softwarebedrijf gaat dit plan verder dan zijn eigen IT-omgeving en moet het plan ook een beleid omvatten over communicatie met klanten en crisisbeheer. Volgens hen zijn veel bedrijven niet goed voorbereid. "Vaak weten ze niet wat te doen", zegt Schütte.

Als IT-systemen worden gehackt, moeten bedrijven ervoor zorgen dat hun diensten zo spoedig mogelijk weer beveiligd en online zijn en dat ze hun klanten ondertussen op competente manier kunnen bedienen.

De toekomst van cybergerelateerde risico's in het digitale tijdperk lijkt dan wel afschrikwekkend, maar geen preventieve maatregelen nemen om je bedrijf te beschermen, is zoals de voordeur wijd open laten staan en hopen dat er niets wordt gestolen. Het is zinvoller om te leren over cyberhygiëne en de nodige voorzorgsmaatregelen in te voeren om u en uw klanten te beschermen.

Eerste contactpersonen

Barry Schütte
Manager Industry Practices Benelux, Chubb
bschutte@chubb.com

Wouter Wissink
Senior Principal Cyber Risk Engineer & Technology Industry Practitioner, Chubb
wwissink@chubb.com

Chubb. Insured.℠

Alles in dit document dient louter algemene, informatieve doeleinden. Het vormt geen persoonlijk advies of aanbeveling van een product of dienst aan enige natuurlijke persoon of onderneming. Kijk in de verstrekte polisdocumenten voor de volledige dekkingsvoorwaarden.

Chubb European Group SE (CEG). Actief in het VK via een bijkantoor gevestigd te 100 Leadenhall Street, London EC3A 3BP. Risico's binnen de Europese Economische Ruimte worden verzekerd door CEG, dat aan de bepalingen van het Franse wetboek van Verzekeringen is onderworpen. Geregistreerd ondernemingsnummer: 450 327 374 Handelsregister Nanterre. Maatschappelijke zetel: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, Frankrijk. Volgestort maatschappelijk kapitaal van € 896.176.662.

NL8224-WA07/22