Henk van Steeg, voormalig CIO Thales Nederland: “Spionnen jagen op onze hightech producten”

Pentesten als wapen tegen cybercrime

Wereldwijd vinden er gemiddeld twee cyberaanvallen per seconde plaats. Tachtig procent daarvan zijn DDoS-aanvallen of bedreiging door ransomware. Begin augustus publiceerde het CBS de laatste cijfers. In Nederland werden in 2021 6.300 bedrijven getroffen door een aanval met ransomware. Grote bedrijven (>10 mld omzet) registreren gemiddeld 50 veiligheidsincidenten per dag met een omzetschade van vijf procent. Dit alles vraagt om een hogere weerbaarheid en betere risico-inventarisatie.

Henk van Steeg is voormalig Chief Information Officer (CIO) bij Thales Nederland

Het grootste deel van de ondernemingen investeert nog steeds reactief, naar aanleiding van een incident. De toename van het aantal incidenten laat zien dat cyberaanvallen meer en eenvoudiger worden opgeschaald, zeker met het toenemend gebruik van AI. Een proactief cyberrisicobeleid is noodzakelijk.

Een van de middelen die ondernemingen kunnen inzetten om de cyberbestendigheid van hun systemen en de mensen die deze systemen gebruiken te onderzoeken, zijn zogeheten pentesten. Bij zo’n penetratietest kruipt een onderzoeker in de huid van een kwaadwillende hacker en probeert toegang te krijgen tot de digitale systemen van een bedrijf. Thales Nederland laat ethische hackers deze testen uitvoeren om te borgen dat de cyberbeveiliging mee-evolueert met de toenemende dreigingen. Thales is een beursgenoteerd technology concern actief in luchtvaart- en defensie-industrie met een jaaromzet van 20 miljard euro. Het bedrijf maakt hightech producten voor met name defensie, maar daarnaast vertrouwen negentien van de twintig grootste banken ter wereld op de systemen van Thales. Deze systemen beschermen tachtig procent van alle online transacties wereldwijd. Het bedrijf heeft een grote, eigen cyberveiligheidsafdeling. Henk van Steeg, voormalig Chief Information Officer (CIO) bij Thales Nederland is duidelijk over het doel van het uitvoeren van pentesten. “We willen elke kwetsbaarheid in onze systemen weten en vinden, ongeacht of het onze website, gebruikte applicaties of de gehele ICT-infrastructuur betreft.”

Pentesten leveren actiepunten

Thales Nederland laat een aantal keer per jaar gepland en ongepland pentesten uitvoeren door zowel een eigen team van pentesters als door externe partijen. Dat is volgens Henk een gezonde mix doordat een externe partij juist niet alle details van de infrastructuur kent. Hij legt uit dat Thales gebruikmaakt van twee soorten pentesten. “De eerste simuleert een bedreiging van binnenuit. Dan openen we ergens in het systeem een poortje en wordt geprobeerd om dieper in het systeem door te dringen. De tweede test is een daadwerkelijke dreiging van buitenaf, waarbij de hacker probeert via het internet bij ons binnen te komen. Beide soorten testen leveren telkens een aantal actiepunten op die zorgen voor een optimalisatie van onze beveiliging.”

> SPIONAGE IS DE GROOTSTE DREIGING WAARMEE THALES TE MAKEN HEEFT

China is ongeëvenaard

De Nationaal Coördinator Terrorismebestrijding en Veiligheid stelt in zijn jaarlijkse Cybersecuritybeeld Nederland dat ‘statelijke actoren in toenemende mate de digitale ruimte structureel en intensief gebruiken voor de behartiging van hun geopolitieke belangen’. China is ongeëvenaard in de schaal waarop en de breedte waarin inlichtingen worden ingewonnen. Spionage is volgens Henk de grootste dreiging waarmee Thales te maken heeft. “Andere landen die onze kennis proberen te stelen om er misbruik van te kunnen maken, vormen de grootste cyberdreiging. DDoS-aanvallen zijn voor ons minder bedreigend. Thales verkoopt high secure systemen. Het is voor onze klanten van groot belang dat deze systemen veilig zijn. Dit is een gespecialiseerde tak van sport.” De oud-CIO vervolgt: “Ik zeg altijd tegen mijn team dat ik me geen zorgen maak over wat ze zien, maar wel om wat ze niet zien. Tot op heden is er nog geen geslaagde ransomware-aanval geweest. Daarvoor was het wel noodzakelijk om het aantal medewerkers op cybersecurity en de investering erin aanzienlijk te verhogen.”

> ZEVENTIG PROCENT VAN ALLE VEILIGHEIDS-INCIDENTEN HEEFT EEN INTERNE OORZAAK

Phishing

Medewerkers, maar ook andere bedrijven in de keten vormen een belangrijk aandachtspunt bij een optimale bedrijfsbeveiliging. Hackers hebben namelijk een manier nodig om systemen binnen te dringen. Het Cybersecurity & Infrastructure Security Agency (CISA) uit de VS schrijft dat ransomware het makkelijkst bij organisaties binnenkomt via e-mailphishing. Ruim veertig procent van alle ransomware-aanvallen zijn te linken aan deze malafide e-mails. Zeventig procent van alle veiligheidsincidenten heeft een interne oorzaak. Thales probeert de medewerkers zoveel mogelijk in te lichten over de resultaten van onder andere de pentesten. Henk: “We vertelden onze personeelsleden dat wat ze gingen horen heel vertrouwelijk was, dat iedereen zijn mobiele telefoon op vliegtuigstand moest zetten en we deden de deur op slot. Dat maakte indruk. De resultaten van zo’n pentest delen, zorgt ervoor dat medewerkers beter weten waarop ze alert moeten zijn.”

Eenvoudig doelwit

Niet alleen de eigen medewerkers moeten zich goed bewust zijn van de gevaren van cyberaanvallen. Dit geldt zoals gezegd ook voor andere bedrijven in de keten van toeleveranciers of afnemers. Leveranciers zijn vaak kleinere bedrijven. Omdat hun ICT-infrastructuur minder complex is en de bestedingen aan cyberveiligheid vaak geringer, zijn zij voor cybercriminelen een eenvoudiger doelwit. Veel bedrijven leggen dan ook in de inkoopvoorwaarden vast dat toeleveranciers bepaalde veiligheidsmaatregelen moeten nemen en dat ook moeten aantonen. Omdat Thales voor het ministerie van defensie werkt, voldoet het bedrijf aan de Algemene Beveiligingseisen Defensieopdrachten (ABDO). Volgens Henk vertaalt Thales deze beveiligingseisen ook weer door naar de veiligheid die ze van hun toeleveranciers eisen en naar de veiligheid van de systemen die ze leveren. Naar aanleiding van een motie in de Tweede Kamer heeft demissionair minister Adriaansens van Economische Zaken en Klimaat toegezegd om in samenwerking met het Digital Trust Center een nieuw keurmerk te laten ontwikkelen door het CCV (Centrum voor Criminaliteitspreventie en Veiligheid).

Dit keurmerk zal zich richten op het certificeren van het werk van ICT-dienstverleners om mkb-organisaties te helpen bij het verhogen van hun cyberweerbaarheid. Het is de bedoeling hiermee het mkb te ondersteunen in het verbeteren van de cyberweerbaarheid van hun organisatie (de 'basis op orde te brengen') door makkelijk een betrouwbare aanbieder te kunnen kiezen.

Grote risico's

Terug naar de pentest als geschikt middel om de eigen digitale veiligheid te onderzoeken en borgen. Veel bedrijven beschikken niet zoals Thales over de kennis om deze testen zelf uit te voeren. Daarmee word je dan afhankelijk van een derde partij. De uitvoerende partij voor pentesten moet betrouwbaar zijn want er gaan grote risico's mee gepaard. De recente cijfers van het CBS tonen eens te meer aan dat het niet meer de vraag is of je bedrijf zal worden aangevallen, maar wanneer. Het is daarom van belang voor zowel grote als kleine ondernemers om de regie te nemen en een actief cyberveiligheidsbeleid op te tuigen. Een pentest door een CCV-gecertificeerd cybersecuritybedrijf is daarbij een goed hulpmiddel om de veiligheid te toetsen. Regelmatig testen borgt ook de veiligheidsaanpak voor de toekomst. In het licht van de verder doorgroeiende digitalisatie en de kwetsbaarheid die daarmee ontstaat voor onze digitale infrastructuur geen overbodige luxe. <

DE VRAAG IS NIET OF MAAR WANNEER JE BEDRIJF ZAL WORDEN AANGEVALLEN

Het CCV-keurmerk Pentesten

Onafhankelijk toezicht op de kwaliteit van pentest-diensten is een belangrijke stap in de strijd tegen cybercriminaliteit. Het Centrum voor Criminaliteitspreventie en Veiligheid heeft daarom, met hulp van een groot aantal belanghebbenden, vorig jaar het CCV-keurmerk Pentesten gelanceerd. Dankzij dit keurmerk kunnen afnemers erop vertrouwen dat de aanbieder van de pentest goed werk levert. De bedrijven die pentesten met keurmerk kunnen leveren zijn te vinden via: https://www.hetccv.nl/pentest

De regering wil in overleg gaan met het Digital Trust Center (DTC) en diverse brancheorganisaties om een eenduidig mkb-keurmerk te ontwikkelen. Dit keurmerk is bedoeld om mkb-organisaties beter te ondersteunen bij het vormen van hun securitybeleid. Hoewel er een voorkeur is voor een Europees keurmerk, is er op nationaal niveau een inventarisatie en consultatie uitgevoerd. Uit deze consultatie bleek dat er vooral behoefte is aan een keurmerk voor ICT-dienstverleners. Dit keurmerk moet laagdrempelig, toegankelijk en betaalbaar zijn. Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) zal een centrale rol spelen in de ontwikkeling, uitgifte en het onderhoud van het keurmerk. Het CCV wordt gezien als een solide keuze en zal nog vóór het einde van dit jaar subsidie ontvangen. De verwachting is dat de ontwikkeling van het keurmerk twee jaar zal duren.