Cybersecurity, een gevecht tegen onzichtbare vijanden

een zaak van een ordelijke interne keuken

VanRoey.be
Tom Hufkens

De dag dat je getroffen wordt door ransomware, zal aanvoelen alsof er een kernbom in het hart van je bedrijf ontploft. Wellicht heb je al een aantal beveiligingstechnologieën geïnstalleerd, om je bedrijf te beschermen tegen kwaadaardige code. Maar – zoals de meeste organisaties – loopt ook jouw bedrijf nog steeds risico. En dat risico kan zowel van buitenaf als van binnenuit komen!

CHANTAGE OP HET INTERNET

Ransomware – of ook gijzelsoftware genoemd - kan o.a. binnen komen via een e-mail of een zogenaamde worm. Het **versleutelt je data** en verstoort op die manier de operaties in je bedrijf. De cybercriminelen vragen **losgeld, in ruil voor het opheffen van de encryptie**.

Middelgrote ondernemingen blijken het meest getroffen. Zij zijn een interessante target voor de hackers, omdat hun IT vaak minder goed beveiligd is dan die van grotere bedrijven. Bovendien is de impact van een cyberaanval op een middelgrote onderneming meestal zwaar genoeg om er toch een aardige som losgeld tegenover te stellen.

DE VIJAND IS NIET ALTIJD GEKEND

Goede **antivirus software** en een betrouwbare **firewall** zijn de voor de hand liggende middelen om ransomware buiten te houden. Antivirus software moet je natuurlijk goed geüpdatet houden, want die updates bevatten de nieuwe bedreigingen die je antivirus provider recent ontdekt heeft. Maar natuurlijk brengen cybercriminelen ondertussen alweer nieuwe ransomware in omloop, die nog niet gekend is!

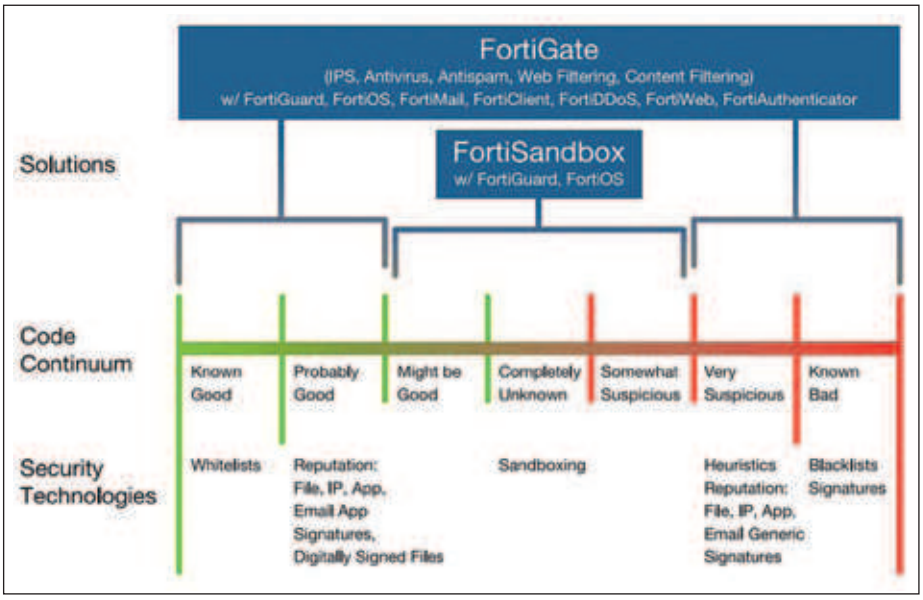
TRADITIONELE BEVEILIGINGSTECHNOLOGIEËN, ZOALS ANTISPAM, WEBFILTERING, IPS, ANTIVIRUS, APP-CONTROLE EN IP-REPUTATIETECHNIEKEN, ZIJN NOODZAKELIJKE BESCHERMINGEN. MAAR ZE ZULLEN DE MEEST GEAVANCEERDE, HEDENDAAGSE AANVALLEN NIET STOPPEN. DAT KOMT OMDAT HUN WERKING GEBASEERD IS OP HET IDENTIFICEREN VAN GEKENDE AANVALSINDICATOREN.

SANDBOXING, EEN EXTRA BESCHERMINGSLAAG

Het gevaar stelt zich dus wanneer een aanval gloednieuw is of zichzelf kan maskeren door middel van tunneling, encryptie of andere ontwijkingsmethodes. Als je sandboxing aan je beveiligingsstrategie toevoegt, dan voeg je een **extra beschermingslaag** toe. En wel één die een kwaadaardige code kan detecteren, zelfs als deze tot nog toe onbekend was.

HOE SANDBOXING WERKT

Bij een verdachte bagagetas in de luchthaven zet men eerst de omgeving af en stuurt men een ontmijningsrobot op de bagagetas af om deze te openen zodat er – ongeacht wat er gebeurt – geen slachtoffers kunnen vallen.
Een sandbox werkt gelijkaardig. **Het**



simuleert de omgeving en het gedrag van echte eindgebruikerssystemen. Er wordt een nieuwe, 100% afgeschermde omgeving opgezet en de – mogelijks kwaadaardige – code wordt uitgevoerd en getest. Nog voor het verdachte bestand in je mailbox verschijnt zal het systeem dat bestand éérst in een afgeschermde omgeving openen en uitgebreid analyseren wat het precies doet.

HOU JE INTERNE KEUKEN OP ORDE

Met de extra bescherming van een sandbox, ben je dus beter gewapend tegen cryptoaanvallen van buitenaf. Helaas ligt de vijand bij vele bedrijven echter intern op de loer.

Achter de versterkte façade wordt er maar al te vaak slordig omgegaan met veiligheidsaspecten. Denk maar aan het gebruik van USB-sticks, third party apps, slecht beheer van toegang en rechten, onbeveiligde PC's, tablets, smartphones en een toenemend aantal IoT devices.

CENTRAAL BEHEER

Steeds meer toestellen zijn verbonden met het bedrijfsnetwerk. Kunnen medewerkers, klanten en leveranciers met hun eigen toestellen veilig op je bedrijfsnetwerk? En hoe zit het met slimme schermen, printers, machines, ...? Een experimentele 3d-printer of zelfs een slim koffiezetapparaat zijn toestellen die gemakkelijk te installeren zijn door proactieve medewerkers. Dat geldt ook voor allerlei handige third party apps. Mooi, met proactieve medewerkers kom je als bedrijf vooruit.

Onderschat het gevaar echter niet als je de controle over het netwerk verliest. Shadow-IT ontsnapt aan de controle van een IT-manager of afdeling. Shadow-IT stelt medewerkers in staat om zelf, snel oplossingen te bedenken voor hun probleem. Vaak gaat het om apps, maar steeds meer ook over smart devices die op je netwerk connecteren.

SECURITY AWARENESS

Alle mensen binnen een bedrijf moeten zich bewust zijn van de gevaren en best practices in hun specifieke rol, met betrekking tot cybersecurity. Security awareness werd vroeger maar al te makkelijk afgeschoven op administratieve en operationele medewerkers die het meest met de IT-systemen in aanraking kwamen. Maar weet jij wat CEO-fraude in de cybersecurity context betekent? Ben jij vertrouwd met social engineering? Cybercriminelen speuren op alle niveaus naar lekken in jouw netwerk.

Het is natuurlijk aan de IT-verantwoordelijke om de juiste tools in gebruik te stellen. Zo kan je bijvoorbeeld met **Multi Factor Authentication** (MFA) een extra beveiliging introduceren bij het inloggen. Dit beschermt je voor een mogelijke hack in het geval je paswoorden dan toch gestolen zijn. Met een proactief **toegangsbeheer** ga je nog een stapje verder. Oplossingen zoals Exabeam laten je toe om de **activiteiten op je netwerk te monitoren** en afwijkend gedrag te onderscheppen. Dat is erg belangrijk, want eenmaal cybercriminelen met ransomware op je netwerk zitten, dan speuren ze daar vaak wekenlang rond alvorens toe te slaan.

MONITORING VAN JE BEDRIJFSNETWERK IS ERG BELANGRIJK, WANT CYBERCRIMINELEN SPEUREN MET RANSOMWARE VAAK WEKENLANG ROND OP JE NETWERK, ALVORENS TOE TE SLAAN.

Cybercriminelen zoeken kleine lekken om in te breken op je netwerk. Het maakt hen weinig uit langs waar ze binnenkomen. Eénmaal op je netwerk, dan vinden ze wel de weg naar de kritische data om die te versleutelen. Een centraal netwerkbeheer is daarom enorm belangrijk.

Ransomware voorkomen is dus een zaak van bedrijfscultuur en gebruik van de juiste tools. De tools zijn vlot beschikbaar en kosten je heus geen arm en een been. Je moet ze uiteraard up-to-date houden. Dat

is dan weer een kwestie van discipline, een onderdeel van een bedrijfscultuur met aandacht voor security.

BACK-UP! EN VERTROUW OP EEN ONDERLEGDE PARTNER

Word je ondanks alles toch nog het slachtoffer van ransomware? Dan kan je maar best de nodige back-ups voorhanden hebben. Die heb je nodig als het misloopt. Worden alle kritische data in jouw bedrijf geback-upt? Worden die back-ups frequent genoeg uitgevoerd? Zijn die back-ups veilig? Een verloren gelegde harde schijf met een verbleekte post-it "back-up" erop volstaat dus niet.

IT is een enorm breed vakgebied. Grote bedrijven beschikken over uitgebreide IT-afdelingen die diverse expertises verenigen. Ook zij doen voor specifieke zaken nog beroep op externe specialisten. Voor kleine en middelgrote ondernemingen is het onmogelijk om al deze kennis in huis op te bouwen. Toch ligt de eindverantwoordelijk over IT en meer specifiek cybersecurity bij één persoon. Vaak is dat de bedrijfsleider, al dan niet bijgestaan door een IT-manager. Laat je daarom bijstaan door een IT-partner met een uitgebreide kennis van security en de nodige oplossingen.

e-book Veilig werken met SVHC/ CMR stoffen

Vereniging ION
Egbert stremmelaar

Het e-book 'Veilig werken met SVHC-/CMR-stoffen' van Vereniging ION is geschreven om het veilig werken met SVHC-/CMR-stoffen aan te moedigen en te ondersteunen. Het maakt duidelijk aan bedrijven dat efficiënt produceren hand in hand gaat met zorgvuldig werken met «gevaarlijke» stoffen.

Ondernemers moeten immers over de juiste informatie en hulpmiddelen (kunnen) beschikken om die veilige werkomstandigheden te creëren.

Het verbieden van het uitvoeren van specifieke werkzaamheden om te kunnen voldoen aan de strenge Europese en nationale milieuregelgeving, is vanuit moreel oogpunt gezien niet altijd acceptabel, omdat we dan onze werkplekproblematiek exporteren naar landen waar de standaard op het gebied van veiligheid (veel) lager is. Beter is het om de stoffen binnen de EU te verwerken onder veilige omstandigheden op basis van een Europese norm of richtlijn.

En als een onderneming eenmaal heeft vastgesteld dat men moet werken met stoffen die onder een autorisatie vallen, dan is ook daar één van de voorwaarden een blootstellingsbeoordeling. Dit e-book geeft richtlijnen over de aanpak.

Het e-book bestaat uit hoofdstukken die openbaar beschikbaar en niet openbaar beschikbaar zijn.

Interesse? Contacteer info@vereniging-ion.nl of bezoek de website https://vereniging-ion.nl/veilig-werken-met-svhc-cmr-stoffen.

Snijbestendige montagehandschoen

Wiltec
Marianne Van Den Haterd

Een snijbestendige handschoen uit de DURACoil serie duwt veiligheid en comfort omhoog. Doordat de snijbestendige vezels van de DURACoil als het ware 'ingepakt' zijn, irriteren deze de huid niet.

De handschoenen voldoen aan de normering EN388:2016 4X43C en zijn verkrijgbaar met diverse coating materialen:

- PU (546) geschikt voor droge werkzaamheden
- foam nitril reliëf (386) geschikt voor werkzaamheden met licht olie of vocht
- geheel olie- en vloeistofdicht door een dubbele nitril coating
- type 576 met een ¾ coating
- type 577 volledig gecoat