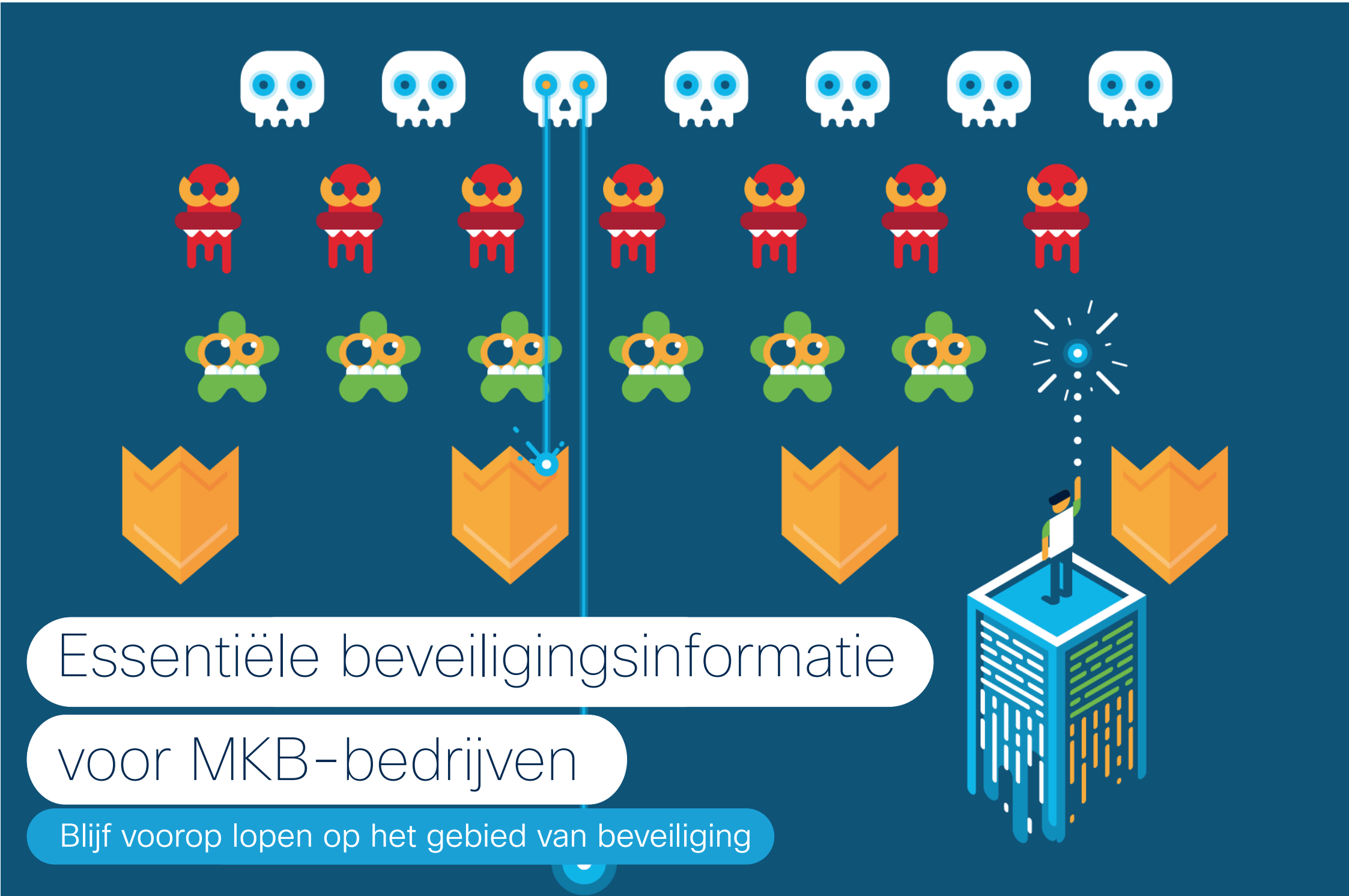
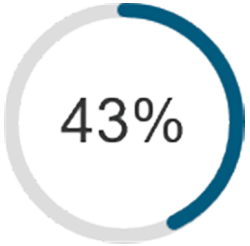


Essentiële beveiligingsinformatie voor MKB-bedrijven

Blijf voorop lopen op het gebied van beveiliging

Leer hoe het huidige MKB-landschap van cyberbedreigingen eruitziet, zodat uw bedrijf kan overleven, operationele kosten kan terugdringen en beveiligd kan groeien. Maak van beveiliging een prioriteit van iedereen en bescherm uw bedrijf met Cisco.

Naarmate uw bedrijf groeit, trekt het de aandacht. Maar niet alle aandacht is welkom. Steeds meer geraffineerde criminele bendes hebben hun pijlen gericht op MKB-bedrijven.



43%
van de cyberaanvallen is gericht op kleine bedrijven. [1]

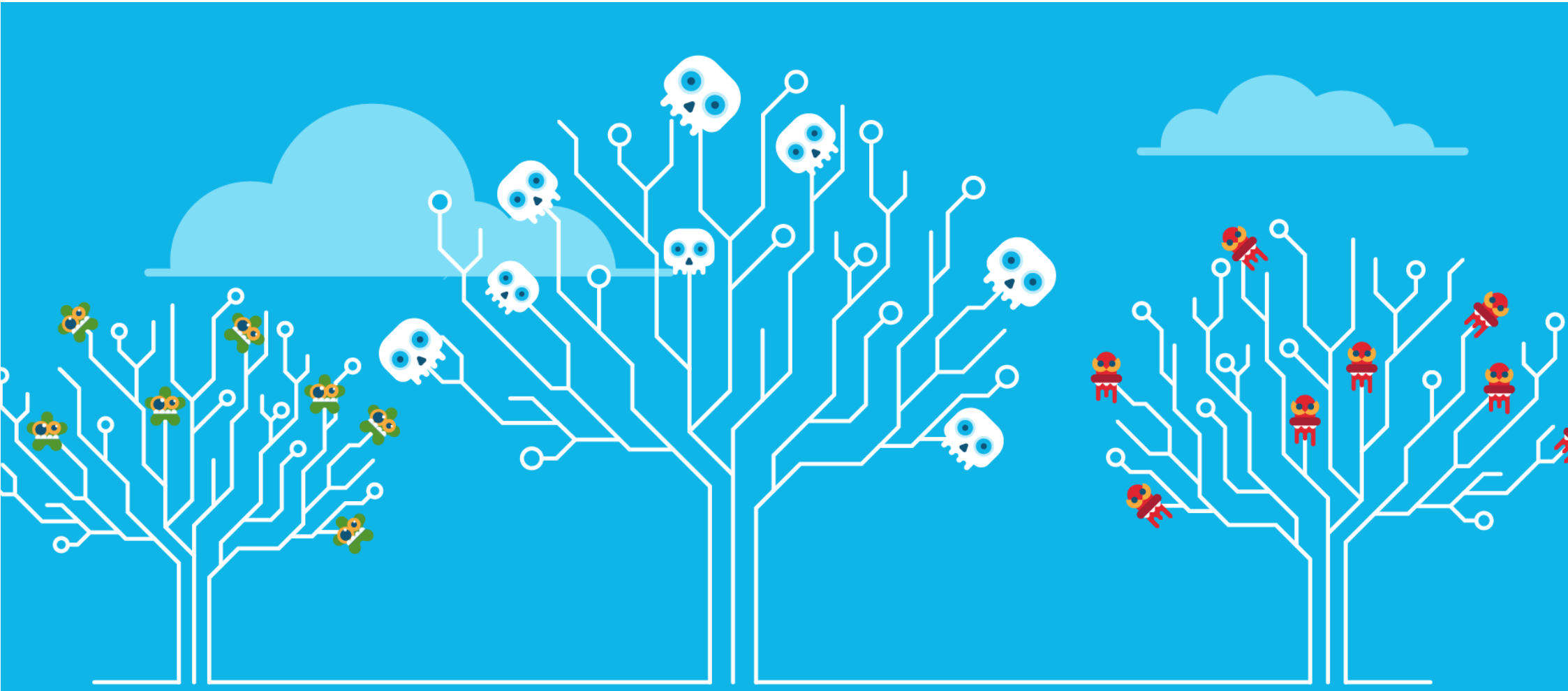
60%
van die bedrijven zal daarna gedwongen zijn te sluiten. [1]

Jaarlijks Cisco Cybersecurity Report 2018 'Cisco ACR 2018'

$ 2.235.018 per jaar

Het bedrag dat MKB-bedrijven gemiddeld besteden na een cyberaanval of gegevensinbreuk om schade of diefstal van IT-middelen te herstellen en na alle verstoringen de normale bedrijfsactiviteiten weer op te pakken.

Het is een bittere waarheid: uw bedrijf kan alleen overleven als u goed begrip hebt van cyberbeveiliging.



Bedreigingen worden steeds geraffineerder

Hackers kennen uw zwakke punten en weten hoe ze deze kunnen misbruiken

De meeste hackers zijn tegenwoordig niet actief 'voor de lol' of om een uitdaging aan te gaan. Zij worden gedreven door geld, zijn goed georganiseerd en werken zelden alleen. Aanvallers zijn flexibel, terwijl bedrijven dat niet altijd zijn. Met name bedrijven die zich op het gebied van beveiliging 'maar behelpen'.

Het doel van een hacker is het stelen van creditcardgegevens, e-mailadressen, gebruikersnamen en wachtwoorden. Alles wat maar aan de hoogste bieder kan worden verkocht. *Hoe* zij dat doen? Zij kunnen de volgende technieken inzetten.

Ransomware

Aanvallers kunnen bedrijven met ransomware virtueel gijzelen, een meedogenloze aanpak. Ransomware versleutelt uw bestanden op afstand zonder uw toestemming. Sommige vormen van ransomware zijn geprogrammeerd om zich over het netwerk te verspreiden.

Er is geen ontvanger meer nodig om een e-mailbijlage te openen of op een koppeling te klikken. Bij de huidige trends in ransomware – zoals WannaCry die in mei 2017 opkwam – wordt kwaadaardige code tussen netwerken verzonden zonder gebruikersinteractie. "WannaCry was de eerste vorm van ransomware die volledig automatisch te werk ging", aldus Craig Williams, Senior Security Outreach Manager bij Talos, Cisco's organisatie voor beveiligingsonderzoek.

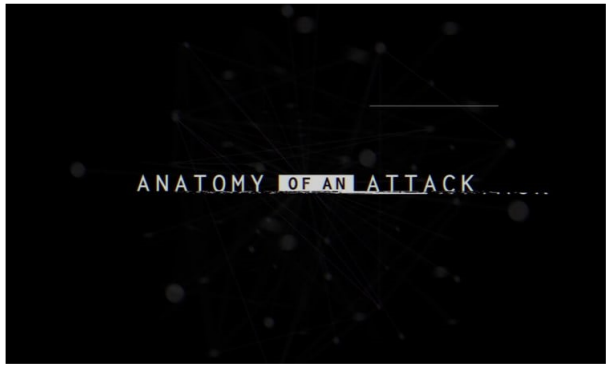
WannaCry trof meer dan 200.000 computers wereldwijd en heeft geleid tot een geschat verlies van $ 4 miljard. WannaCry kan worden geïnstalleerd dankzij een kwetsbaarheid in het SMB-protocol van Microsoft en is met name effectief in oudere Windows-omgevingen, zoals Windows XP, Windows Server 2003 en Windows 8. Microsoft had al een beveiligingsupdate uitgebracht om deze kwetsbaarheid te patchen, maar niet alle gebruikers waren automatisch beschermd.

MKB-bedrijven gegijzeld

52% van de MKB-bedrijven die in 2017 deelnamen aan het onderzoeksrapport 'State of Cybersecurity in Small and Medium-Sized Businesses (SMB)' van het Ponemon Institute had tijdens een periode van 12 maanden te maken gehad met een al dan niet succesvolle ransomwareaanval. Zodra de besmetting is uitgevoerd, wordt een bericht op uw scherm weergegeven waarin wordt geëist dat u losgeld in bitcoins betaalt voor vrijgave van uw gegevens. Het geëiste losgeld bedraagt doorgaans € 200 tot 10.000, maar sommige slachtoffers hebben aanzienlijk meer moeten betalen.
Recente krantenkoppen laten zien dat een nieuwe generatie bedreigingen op wereldwijde schaal viraal gaat en zich sneller dan ooit verspreidt. Cisco's Talos Group voor bedreigingsonderzoek ontdekte de bedreiging VPNFilter die meer dan 500.000 routers voor kleine kantoren/

thuiskantoren en op het netwerk aangesloten opslagapparaten (NAS) wereldwijd besmette. Cisco-apparaten werden niet besmet. Met deze complexe bedreiging kunnen kwaadwillenden verkeer inspecteren dat via de apparaten loopt, bestanden stelen van netwerkback-upschijven en potentieel toegang verkrijgen tot aangesloten bedrijfsnetwerken.

Cybercriminelen begrijpen hun doelwitten, van hun voor- en afkeuren tot de manier waarop zij zaken doen. Ze weten dat hun slachtoffers zullen betalen om hun gegevens vrij te laten geven, en ze maken genadeloos misbruik van elke zwakke plek die ze vinden.



Business Email Compromise (BEC)

Business Email Compromises (BEC's) zijn 75% winstgevender dan ransomware. Toch krijgen BEC-aanvallen minder publiciteit.

BEC-scams zijn gerichte aanvallen waarbij hackers gebruikmaken van social engineering om mensen ertoe aan te zetten geld naar hen over te maken. Er is geen sprake van malware, er zijn geen bijlagen. In tegenstelling tot ransomwareaanvallen worden er geen gegevens van de slachtoffers gestolen. Het draait allemaal om leugens en misleiding.

Hackers besteden veel tijd aan het onderzoeken van hun doelwit en stellen een profiel op. Nadat ze voldoende informatie hebben verzameld, kunnen ze e-mails (spear phishing) sturen naar senior personeelsleden, vaak werkzaam op de financiële afdeling. Ze richten zich op iemand die bevoegd is om geld over te maken. Hoe groter het bedrijf, hoe meer geld ze kunnen binnenhalen. Het aantal aanvallen gericht op kleine en middelgrote bedrijven neemt echter toe.

Hoe groter het bedrijf, hoe meer geld ze kunnen binnenhalen. Het aantal aanvallen gericht op kleine en middelgrote bedrijven neemt echter toe.

Gegevensinbreuk

Gegevens vormen de ruggengraat van uw bedrijf: uw intellectuele eigendom, uw volgende grote doorbraak, uw klantgegevens en uw omzet staan op het spel. Een inbreuk houdt veel meer in dan alleen uitvallende en beschadigde systemen herstellen.

Door een sterk beveiligingspostuur te creëren, kunt u uw intellectuele eigendom en uw reputatie beschermen. Organisaties doen er gemiddeld 191 dagen over om een inbreuk te detecteren, en 66 dagen om deze in te perken (bron: Ponemon Institute). De sleutel om de schade te beperken is echter vroegtijdige detectie.

De mediane detectietijd van Cisco is 3,5 uur. Als een inbreuk plaatsvindt, kunnen experts van Cisco Incident Response Services binnen enkele uren op locatie zijn om u te helpen deze te beperken en de hoofdoorzaken ervan te verhelpen.

Aanvallen op de toevoerketen

Aanvallen op de toevoerketen zijn een opkomende en groeiende cyberbedreiging en tonen aan hoe ervaren cybercriminelen zijn geworden. Kwaadwillenden besmetten de mechanismen (van anderszins legitieme softwarepakketten) die verantwoordelijk zijn voor software-updates. Vervolgens laten ze deze mechanismen 'meeliften' bij de distributie van legitieme software.

De cybercriminelen richten zich op een bedrijf in de toevoerketen met zwakke cyberbeveiligings-praktijken – met name waar het de beveiliging bij het delen van gegevens betreft. Daarom zijn vaak MKB-bedrijven het doelwit.

Zodra de aanvaller de zwakke schakel in de keten heeft geïdentificeerd, kan deze zich richten op het misbruiken van het uiteindelijke beoogde doelwit.

Verdedig u tegen aanvallers, overal

Laat aanvallers uw bedrijf niet op een zijspoor zetten. Richt uw aandacht op alle plekken waar deze maar proberen binnen te komen. Onze oplossingen beschermen u, van de DNS-laag tot e-mail en endpoints. Bovendien wordt gebruikgemaakt van toonaangevend bedreigingsonderzoek van Talos.

Wat te doen

Als u onderdeel uitmaakt van een toevoerketen, vraag dan uw leveranciers/partners hoe zij hun toevoerketen beveiligen. Vraag naar hun ontwikkelingspraktijken en hun interne beveiligingsmechanismen. Hoe rollen ze patches en updates uit naar hun interne systemen, en hoe vaak? Hoe segmenteren en beveiligen zij hun ontwikkelings-, kwaliteits- en productieomgevingen? Hoe lichten zij hun partners en leveranciers door?

En stel deze vragen ook ten aanzien van uw eigen organisatie, anders zou kunnen blijken dat uw bedrijf de zwakste schakel in de toevoerketen vormt.

Meer informatie over aanvallen op toevoerketens: https://gblogs.cisco.com/uki/protecting-...

Te veel bedrijven hebben een ‘stackingprobleem’

Sommige bedrijven hebben geen duidelijke cyberbeveiligingsstrategie: ze volstaan met een oplossing totdat deze een belemmering gaat vormen.

Andere proberen alles te beveiligen en krijgen daardoor te kampen met een stackingprobleem, waarbij de stack bestaat uit diverse deeloplossingen van verschillende leveranciers. Beide situaties leiden tot problemen.

De lappendeken aan incompatibele beveiligingstechnologieën biedt ruimte voor hiaten, zorgt voor beheerproblemen en resulteert in inefficiëntie waar hackers misbruik van maken. Elke nieuwe beveiligingsoplossing heeft weer een andere beheerinterface. Elke nieuwe oplossing vereist de inzet van personeel, beheeruren voor het instellen ervan, het opzetten van beleid, het reageren op waarschuwingen, enzovoort. En het is niet altijd duidelijk of de resulterende extra beveiliging alle tijd en moeite wel waard is die u steekt in het beheren van die oplossing in plaats van u te richten op grotere problemen elders.

Mogelijk hebt u complexiteit toegevoegd zonder dat dit heeft geleid tot algehele incrementele effectiviteit. Het feit dat beveiliging nog steeds wordt beschouwd als primair een ‘IT-kwestie’ maakt de situatie er niet beter op. Volgens de Cisco Security Capabilities Benchmark Study zijn enkele organisaties het er niet meer eens dat managers van bedrijfsonderdelen worden betrokken bij beveiliging. Al te vaak wordt gedacht: ‘Beveiliging is een zaak van de IT-afdeling’. Dit is een groot probleem omdat hierdoor beveiliging vaak wordt toegevoegd aan in plaats van geïntegreerd in het ecosysteem van een bedrijf. Kort door de bocht betekent meer werk.

Bij een goede aanpak kan beveiliging een strategisch bedrijfsmiddel vormen. Een platform voor groei.

Het ‘aanvalsgebied’ wordt groter en gecompliceerder

We werken overal: thuis, op kantoor, in luchthavens en koffiebars. Maar traditionele beveiligingsoplossingen zijn nog steeds gericht op het alleen beschermen van werknemers op het moment dat deze gebruikmaken van het zakelijke netwerk.

Stel u het volgende scenario voor:

– Gebruikers maken verbinding met uw netwerk via hun eigen slimme apparaten, waar ze zich ook maar bevinden

– Uw zakelijke apps, servers en gegevens bevinden zich in de cloud

– Apparaten die niet eens lijken op computers maken verbinding met uw netwerken (zoals slimme meters, thermostaten, printers en camera’s)

– En om het nog ingewikkelder te maken, moet u bepalen hoe u beveiliging overal kunt toepassen om deze complexe infrastructuur te beveiligen

Schaduw-IT

Schaduw-IT is de praktijk waarbij werknemers elke gewenste toepassing gebruiken zonder goedkeuring van de IT-afdeling te verkrijgen. Dit kan van alles omvatten, van de installatie van een instant messenger-service op een werkapparaat tot het downloaden van eigen software voor bestandsdeling en deze gebruiken om gevoelige gegevens over te dragen.

Van de respondenten die in 2017 deelnamen aan het onderzoeksrapport 'State of Cybersecurity in Small and Medium-Sized Businesses (SMB)' van het Ponemon Institute en te maken hadden gehad met een gegevensinbreuk, gaf 54% aan dat onzorgvuldig te werk gaande werknemers de hoofdoorzaak daarvan was. Het jaar ervoor was dat nog 48%.

Schaduw-IT kan tot enorme kwetsbaarheden in de beveiliging leiden, met name als u de reikwijdte van het probleem niet onderkent. Deze situatie is als zwemmen in water vol haaien terwijl u een vleespak draagt. En toch is dit een wijdverspreide praktijk. Waarom?

Om werknemers recht te doen: het gebeurt met de beste bedoelingen. Zij willen hun eigen productiviteitsniveau verbeteren en gebruiken daartoe de nieuwste digitale tools. Meestal denk zij niet na over de beveiligingsimplicaties wanneer zij deze toepassingen gebruiken. Soms gebruiken werknemers schaduw-IT-tools omdat deze in hun vorige organisatie bij bepaalde systemen werden gebruikt. Dat is tenslotte eenvoudiger dan een nieuwe tool leren gebruiken.

Belicht schaduw-IT

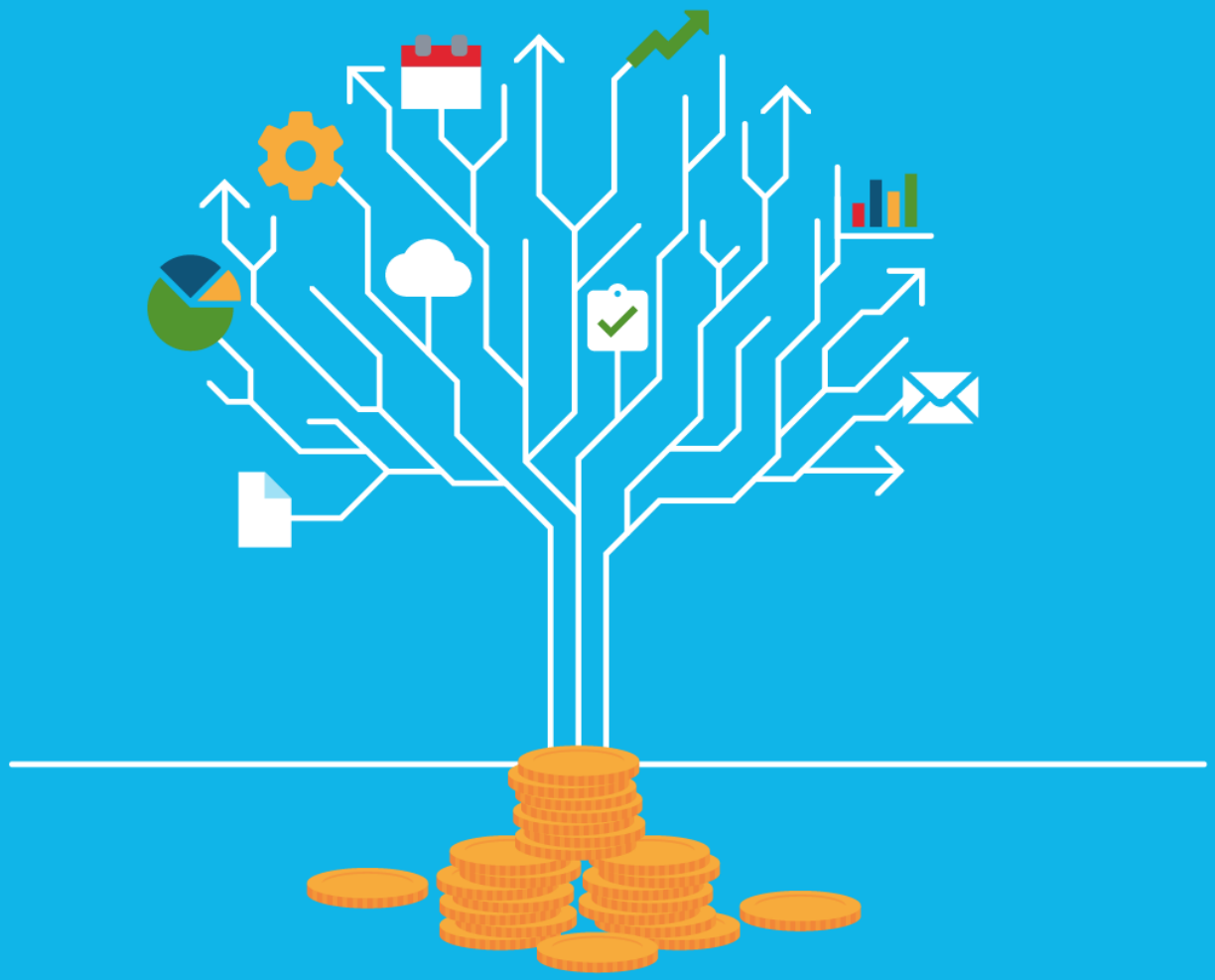
U kunt schaduw-IT een positieve bijdrage laten leveren aan uw bedrijf:

- Zet een forum op of gebruik een 'ideeënbus'-tool waarmee uw werknemers ideeën kunnen indienen om de bedrijfsvoering te verbeteren (als u dat niet al hebt gedaan). Beloon de indieners en vier het wanneer een idee realiteit wordt.
- Effectieve beveiliging gaat niet alleen om de technologie – het gaat ook om het instellen van de juiste processen. Maak van beveiligingsbewustzijn een kernonderdeel van uw trainingsprogramma, zodat werknemers de gevolgen van het gebruik van onbeveiligde apparaten en programma's onderkennen.
- Kennis van wat er in uw netwerk gebeurt is een enorme prioriteit bij IT-beveiliging. Helaas weten de meeste bedrijven niet wanneer een inbreuk heeft plaatsgevonden, hoe de hackers zijn binnengekomen of hoe groot de schade is. Dat moet veranderen.

Wachtwoordbeleid

Sterke wachtwoorden blijven essentieel bij MKB-cyberbeveiliging. Toch gaf 59% van de respondenten die deelnamen aan het Ponemon-onderzoeksrapport aan geen zichtbaarheid te hebben van de wachtwoordpraktijken van hun werknemers, inclusief het gebruik van unieke of sterke wachtwoorden. Dit is hetzelfde percentage als bij het vorige rapport.

Respondenten gaven ook aan dat wachtwoordbeleid niet altijd strikt wordt gehandhaafd. Van de bedrijven die een wachtwoordbeleid hebben (43% van de respondenten), gaf 68% aan dat het beleid niet strikt wordt gehandhaafd of niet zeker weet hoe goed het beleid wordt toegepast.



Groei vereist beveiliging

Zwakke cyberbeveiliging gaat ten koste van innovatie

Het afweren van cyberaanvallen is van groot belang, maar een groter gevaar van een zwakke cyberbeveiliging is de impact ervan op bedrijfsgroei en innovatie.

Tijdens een recent onderzoek van Cisco gaf maar liefst 71% van de leidinggevenden aan dat zorgen ten aanzien van cyberbeveiliging innovatie bij hun bedrijf in de weg zaten. 39% van de respondenten gaf aan bedrijfskritische initiatieven te hebben stopgezet vanwege problemen met de cyberbeveiliging. Hieruit blijkt dat een zwakke cyberbeveiliging het vermogen van bedrijven om te innoveren belemmert, net op het moment dat innovatie juist nodig is om te kunnen concurreren.

Digitalisering, disruptie en exponentiële verandering zijn inmiddels normaal in een zeer concurrerende bedrijfsomgeving. Flexibele bedrijven kunnen een flinke voorsprong nemen op de concurrentie door te innoveren, snel te bewegen en experimenten te belonen.

Een inbreuk heeft niet alleen impact op het bedrijfsresultaat

Als u uw netwerk niet beveiligd, kan dat verstrekkende gevolgen hebben. Denk hierbij aan uitvaltijd, schade aan en vervanging van apparatuur, respons op incidenten, forensisch onderzoek, interne audits en communicatie.

Verlies van klantvertrouwen kan een voorheen goede inkomstenbron permanent schaden. Verlies van klantgegevens kan resulteren in juridische acties, boetes, verscherpte regelgeving en herstelkosten. En dat is nog niet alles. Als een detailhandelaar bijvoorbeeld te maken krijgt met een gegevensinbreuk, willen klanten mogelijk liever geen persoonsgegevens meer delen.

Uw bedrijf kan doorslaggevend voordeel behalen door gebruik te maken van de volgende middelen:

– Gevestigde technologieën zoals web, mobiel, cloud, Enterprise Resource Planning (ERP) en Customer Relationship Management (CRM)

– Snel ontwikkelende technologieën zoals kunstmatige intelligentie en gegevensanalyse

Met deze technologieën kunnen bedrijven beter in contact komen met hun klanten, nieuwe markten bereiken, de productiviteit van werknemers vergroten en tegelijkertijd inkomsten verhogen en kosten verlagen. Zorgen over cyberbeveiliging kunnen de implementatie van enkele digitale bedrijfsmodellen en innovaties belemmeren.

Het dilemma van de keuze

Veel zakenmensen staan voor een lastige keuze. Ze lopen het risico een verkeerde keuze te maken

of achter te blijven. Ze zijn van mening dat ze zich moeten blijven ontwikkelen om niet door digitale disruptors en andere flexibele concurrenten te worden voorbijgestreefd. 73% van onze respondenten gaf aan vaak nieuwe technologieën en bedrijfsprocessen te implementeren, ondanks de cyberbeveiligingsrisico's.

Bedrijven waar de cyberbeveiliging onder de maat is hebben de slechtst mogelijke concurrentiepositie: zij innoveren niet snel genoeg om concurrerend te zijn, maar zijn toch niet genoeg beschermd tegen cyberaanvallen, ondanks dat zij digitale innovaties uitstellen.

Wat zou de impact van een beveiligingsinbreuk of ransomwareaanval op uw bedrijf zijn?

Wat is de potentiële financiële impact van netwerkuitval als gevolg van een beveiligingsinbreuk? Of als u geen toegang meer hebt tot gegevens en systemen als gevolg van een ransomwareaanval?

- Zou een beveiligingsinbreuk of ransomwareaanval uw toevoerketen kunnen verstoren?
- Wat zou er gebeuren als uw website door een aanval uit de lucht ging?
- Maakt uw bedrijf op de website gebruik van e-commercefuncties?
- Hoe lang kan de site uit de lucht blijven voordat het uw bedrijf geld gaat kosten?
- Is uw bedrijf verzekerd tegen cyberaanvallen of tegen misbruik van de gegevens van uw klanten? Is deze verzekering afdoende?
- Heeft uw bedrijf back-up- en herstelmogelijkheden om informatie na een beveiligingsinbreuk of ransomwareaanval eventueel terug te zetten?

Potentiële digitale waarde

Op basis van de potentiële digitale waarde wordt een waarde toegekend aan beveiliging. Deze waarde wordt gebaseerd op geheel nieuwe bronnen van waarde afkomstig van digitale investeringen en innovaties, en waardeverschuivingen tussen bedrijven op basis van hun vermogen om digitale mogelijkheden te benutten.

Een deel van de potentiële digitale waarde is afkomstig van de defensieve kant van cyberbeveiliging, zoals:

- Bescherming van intellectueel eigendom
- Afname van het aantal besmette gegevens (zowel interne als klantinformatie), toename van bedrijfsuptime en afname van netwerkuitval
- Bescherming van financiële bedrijfsmiddelen
- Bescherming van gevoelige overheids-/nationale/politieke informatie
- Behoud van bedrijfsreputatie

Verkrijg een volledig beeld. Lees Cisco's e-book The Ultimate Guide to Cybersecurity to Drive Profitability.

Een beveiligd platform voor groei

Cisco's geïntegreerde beveiligingsarchitectuur ondersteunt bedrijven: bij het verbeteren van de beveiligingseffectiviteit door de detectietijd van bedreigingen te verkorten en incidenten op te lossen, bij het stimuleren van besparingen (zowel op het gebied van kapitaalbehoeften als operationele uitgaven) en bij het verbeteren van de productiviteit van IT-personeel.

Alle neuzen dezelfde cyberbeveiligingskant op

Maak van beveiliging een prioriteit voor iedereen

Soms is er een schok nodig voordat cyberbeveiligingsinitiatieven doorgang vinden.

60% van de MKB-bedrijven die te maken krijgen met een cyberbeveiligingsinbreuk, moet het bedrijf sluiten. Dit betekent dat, met name voor u, voorkomen beter is dan genezen.

Presenteer de specifieke risicofactoren voor uw bedrijf

Help uw directie te begrijpen welke beveiligingsbedreigingen uw specifieke organisatie kunnen schaden. Besteed niet te veel tijd aan het presenteren van algemene trends en statistieken. Help hen in plaats daarvan de verbinding te zien tussen die beveiligingstrends en de uitdagingen die specifiek van toepassing zijn op uw bedrijf en branche. Hoe meer context u kunt geven, hoe relevanter het voor uw directie zal zijn.

U kunt het bijvoorbeeld hebben over de grootste bron van inkomsten van uw bedrijf en voorbeelden geven van de manier waarop beveiligingsbedreigingen zoals ransomware die in gevaar brengen. Als uw bedrijf gevoelige gegevens zoals financiële gegevensrecords bewaart, kunt u voorbeelden laten zien van de juridische gevolgen en boetes voor uw bedrijf als dergelijke gegevens openbaar worden gemaakt.

Laat hen zien hoe een aanval werkt, hoe eenvoudig het kan zijn de beveiliging in gevaar te brengen. Geef ze echte voorbeelden van de kwesties waar u al meet te maken hebt, naast de risico's en mogelijk effecten op de lange termijn van dergelijke problemen.

Kwantificeer alles

Leidinggevenden houden van meetcriteria en cijfers. Daarom is het belangrijk dat u uw beveiligingsprioriteiten op een lijn stelt met de doeleinden en deadlines van uw bedrijf. Bevestig hun zakelijke en IT-prioriteiten en laat zien hoe beveiliging kan helpen deze te bereiken.

Geef ook de keerzijde weer: hoe een beveiligingsincident een risico kan vormen voor hun plannen. Bijvoorbeeld: als u op het punt staat een nieuw product uit te brengen, wat is de potentiële schade voor uw bedrijf als dat intellectuele eigendom openbaar wordt gemaakt of vernietigd?

Het hoeft in feite geen hypothetische kwestie te zijn. Het is een nog beter argument als u kunt kwantificeren wat bestaande beveiligingsproblemen het bedrijf al kosten.

Herhaal, herhaal, herhaal

Het is onwaarschijnlijk dat een enkele bespreking u alles geeft wat u nodig hebt. Maak uw communicatie eenvoudig en frequent. Praat regelmatig bij en rapporteer vaak op relevante meetcriteria. Wees niet bang in herhaling te vallen en probeer verschillende invalshoeken tot de boodschap overkomt en u de fondsen en steun krijgt die u nodig hebt.

Hoe GDPR zal helpen

In veel gevallen vinden beveiligingsprofessionals het moeilijk om de taal van de directie te spreken en hen te helpen te begrijpen waarom investeringen in beveiliging prioriteit moeten krijgen. De redenen voor investering worden kristalhelder als leidinggevenden na een cyberaanval de multidimensionale schade zien die deze veroorzaakt. Gesprekken (en veranderingen) gaan een stuk sneller als iedereen de kwestie begrijpt.

Daarom kan wetgeving zoals de General Data Protection Regulation (GDPR), die in mei 2018 van kracht werd, helpen bij het verbeteren van de beveiliging.

Bedrijven die al in beveiliging investeren hebben waarschijnlijk niet veel om zich zorgen over te maken, aangezien zij al aardig op weg zijn qua naleving (voor de beveiligingskant van de GDPR). Aan de andere kant kan de GDPR, voor die organisaties die worstelen met het vrijmaken van geld voor investeringen, een uitgelezen kans bieden om beveiligingsprofessionals en leiding op een lijn te krijgen. Dit soort nieuwe wetgeving legt minimale eisen op aan bedrijven, hetgeen in de toekomst zal helpen grotere technologische innovatie te ondersteunen.

Gegevensprivacy en IT-beveiliging zijn niet alleen voorschriften, maar ook de vraag van de klant. Bedrijven krijgen steeds frequenter vragen van hun klanten over de omgang met hun gegevens. Er is een vertrouwensrelatie, een aanname dat het bedrijf dat hun gegevens ontvangt er goed mee zal omgaan. De wet is er alleen om ervoor te zorgen dat bedrijven alles doen om dat vertrouwen niet te beschamen.

Bescherm uw bedrijf met Cisco

Netwerkbeveiliging

Wat is netwerkbeveiliging?
Netwerkbeveiliging omvat elke activiteit die is bedoeld om de bruikbaarheid en integriteit van uw netwerk en gegevens te beschermen. Dit betreft zowel hardware- als softwaretechnologieën. Met effectieve netwerkbeveiliging wordt de toegang tot het netwerk beheerd. Hierbij worden diverse bedreigingen gestopt zodat deze zich niet verder kunnen verspreiden op uw netwerk en hackers geen toegang krijgen.

Hoe werkt netwerkbeveiliging?
Bij netwerkbeveiliging worden meerdere beveiligingslagen bij de edge en in het netwerk gecombineerd. Op elke netwerkbeveiligingslaag worden beleidsregels en controles geïmplementeerd. Geautoriseerde gebruikers krijgen toegang tot netwerkresources, maar kwaadwillenden worden geblokkeerd zodat ze geen exploitaties en bedreigingen kunnen uitvoeren.

Hoe profiteer ik van netwerkbeveiliging?

Digitalisering heeft onze wereld, onze manier van leven, werken, spelen en leren, getransformeerd. Elke organisatie die de services wil leveren waar klanten en werknemers om vragen, moet zijn netwerk en eigendomsinformatie beschermen tegen aanvallen. Uiteindelijk beschermt u daarmee uw reputatie.

Zes stappen om uw netwerk te beveiligen

1. Bewaak het via de firewall binnenkomende en uitgaande verkeer en neem de gemelde kwesties zorgvuldig door. Vertrouw niet op waarschuwingen om gevaarlijke activiteiten te markeren. Zorg dat iemand van uw team de gegevens begrijpt en de nodige actie kan ondernemen.
2. Blijf alert op nieuwe bedreigingen die worden ontdekt en online worden gepost. Via de Cisco Talos-blog worden bijvoorbeeld directe updates gegeven over nieuwe bedreigingen, kwetsbaarheden en een gedetailleerd wekelijks overzicht van bedreigingen. Op de TrendWatch-site van Trend Micro worden actuele bedreigingsactiviteiten gevolgd. U kunt ook het Amerikaanse Computer Emergency Readiness Team (US-CERT) u e-mailwaarschuwingen laten sturen over recent bevestigde softwarekwetsbaarheden en exploitaties.
3. Voer regelmatig updates uit van uw firewall- en antivirussoftware.
4. Geef werknemers regelmatig training zodat zij op de hoogte zijn van eventuele wijzigingen in uw beleid voor aanvaardbaar gebruik. Stimuleer ook een ‘buurtwacht’-aanpak van beveiliging. Als een werknemer iets verdachts opmerkt (hij/zij kan zich bijvoorbeeld niet direct aanmelden bij een e-mailaccount), moet deze de juiste persoon hiervan onmiddellijk op de hoogte stellen.
5. Installeer een oplossing voor gegevensbescherming. Dit type apparaat kan uw bedrijf beschermen tegen gegevensverlies als er sprake is van een inbreuk op de netwerkbeveiliging.
6. Overweeg de inzet van aanvullende beveiligingsoplossingen om uw netwerk verder te beschermen en de mogelijkheden van uw bedrijf uit te breiden.

Typen netwerkbeveiliging

Toegangscontrole

Niet elke gebruiker zou toegang tot uw netwerk moeten hebben. Om potentiële aanvallers buiten te houden, moet u elke gebruiker en elk apparaat kunnen herkennen. U kunt dan uw beveiligingsbeleid afdwingen. U kunt endpointapparaten die niet aan het beleid voldoen, blokkeren of slechts beperkte toegang verlenen. Dit proces wordt netwerktoegangsbeheer (NAC) genoemd.

Toepassingsbeveiliging

Alle software die wordt gebruikt bij het uitvoeren van uw bedrijfsactiviteiten moet worden beschermd, ongeacht of de software door uw IT-personeel is ontwikkeld of door u is gekocht. Toepassingen kunnen echter 'gaten' (kwetsbaarheden) bevatten die aanvallers kunnen misbruiken om uw netwerk te infiltreren. Toepassingsbeveiliging omvat de hardware, de software en de processen die u gebruikt om die gaten te dichten.

Antivirus- en antimalwareprogramma's

Malware (afkorting van 'malicious software', kwaadaardige software) omvat virussen, wormen, trojans, ransomware en spyware. Soms kan malware een netwerk besmetten en vervolgens dagen of zelfs weken sluimerend aanwezig blijven. De beste antimalwareprogramma's scannen niet alleen op malware op het moment dat deze binnendringt, maar blijven bestanden ook daarna volgen om abnormaliteiten te detecteren, malware te verwijderen en schade te herstellen.

Voorkoming van gegevensverlies

Organisaties moeten ervoor zorgen dat hun werknemers geen gevoelige informatie buiten het netwerk verzenden. Technologieën ter voorkoming van gegevensverlies (DLP) kunnen helpen voorkomen dat cruciale informatie op een onveiligemanier wordt geüpload, doorgestuurd of zelfs afgedrukt.

Gedragsanalyses

Om abnormaal netwerkgedrag te kunnen detecteren, moet u eerst weten wat normaal netwerkgedrag is. Met tools voor gedragsanalyse worden activiteiten die afwijken van de norm automatisch gedetecteerd. Uw beveiligingsteam kan vervolgens aanwijzingen van besmetting die een potentieel probleem vormen, beter identificeren en bedreigingen snel verwijderen.

E-mailbeveiliging

E-mailgateways vormen de belangrijkste bedreigingsvector voor een beveiligingsinbreuk. Aanvallers gebruiken persoonlijke informatie en social engineeringtechnieken om geraffineerde phishingcampagnes op te zetten om ontvangers te misleiden en naar sites met malware te sturen. Met een toepassing voor e-mailbeveiliging worden inkomende aanvallen geblokkeerd en worden uitgaande berichten gecontroleerd om verlies van gevoelige gegevens te voorkomen.

Firewalls

Firewalls vormen een barrière tussen uw vertrouwde interne netwerk en niet-vertrouwde externe netwerken, zoals het internet. Hierbij wordt

een set gedefinieerde regels gebruikt om verkeer toe te laten of te blokkeren. Een firewall kan hardware, software of beide zijn. Cisco biedt UTM-apparaten (Unified Threat Management) en bedreigingsgerichte firewalls van de volgende generatie.

Inbraakpreventiesystemen

Een inbraakbeveiligingssysteem (IPS) scant netwerkverkeer om aanvallen actief te blokkeren. Cisco NGIPS-applicaties (Next-Generation IPS) doen dit door enorme hoeveelheden wereldwijde bedreigingsinformatie te correleren en niet alleen kwaadaardige activiteit te blokkeren, maar ook de voortgang van verdachte bestanden en malware te volgen over het netwerk om de verspreiding van uitbraken en herinfectie te voorkomen.

Beveiliging van mobiele apparaten

Cybercriminelen richten hun pijlen steeds meer op mobiele apparaten en apps. Binnen de komende drie jaar zal 90% van de IT-organisaties zakelijke toepassingen op persoonlijke mobiele apparaten ondersteunen. Natuurlijk moet u kunnen bepalen en controleren welke apparaten toegang hebben tot uw netwerk. En u moet hun verbindingen configureren om netwerkverkeer privé te houden.

Netwerksegmentering

Met softwaregedefinieerde segmentering wordt het netwerkverkeer geclassificeerd, waardoor het handhaven van beveiligingsbeleid eenvoudiger wordt. Idealiter worden de classificaties gebaseerd op de identiteit van endpoints, niet alleen op IP-adres. U kunt toegangsrechten verlenen op basis van rol, locatie en meer, zodat het juiste toegangsniveau wordt toegewezen aan de juiste personen en verdachte apparaten worden ingeperkt en hersteld.

VPN

Bij een virtueel particulier netwerk (VPN) wordt de verbinding met een netwerk via een endpoint, vaak via het internet, versleuteld. Bij een VPN voor externe toegang wordt gebruikgemaakt van IPsec of Secure Sockets Layer om de communicatie tussen apparaat en netwerk te verifiëren.

Webbeveiliging

Met een webbeveiligingsoplossing wordt het webgebruik van uw werknemers beheerd, worden webgebaseerde bedreigingen geblokkeerd en wordt toegang tot kwaadaardige websites geweigerd. Uw webgateway op locatie of in de cloud wordt beschermd. ‘Webbeveiliging’ heeft ook betrekking op de stappen die u neemt om uw eigen website te beschermen.

Draadloze beveiliging

Draadloze netwerken zijn minder beveiligd dan bekabelde. Zonder strenge beveiligingsmaatregelen is het installeren van een draadloos LAN net zoiets als overal Ethernet-poorten plaatsen (inclusief parkeerplaats). Om succesvolle exploitaties tegen te gaan, moet u producten gebruiken die speciaal zijn ontwikkeld om een draadloos netwerk te beschermen.

Talos-bedreigingsinformatie

Cisco’s Talos Security Intelligence and Research Team is toonaangevend binnen de branche en elk Cisco-beveiligingsproduct wordt via Talos beschermd. Wereldwijd zijn meer dan 250 bedreigingsonderzoekers dag en nacht actief, en Talos heeft een opslagplaats met 100 terabyte aan bedreigingsinformatie.

Het team ziet dagelijks een derde van het wereldwijde e-mailverkeer en meer dan 2% van de wereldwijde DNS-aanvragen. Het verwerkt dagelijks 1,1 miljoen unieke malwaresamples via onze AMP- (Advanced Malware Protection) en Threat Grid-technologie waarmee dagelijks 19,7 miljard bedreigingen op de netwerken van onze klanten worden geblokkeerd.

U leest het goed: dagelijks worden 19,7 miljard bedreigingen geblokkeerd.

Deze enorme kennis en onderzoeksmogelijkheden waarborgen Cisco's cyberbeveiligingsoplossingen die de zichtbaarheid, automatisering, flexibiliteit en schaalbaarheid bieden die nodig zijn om uw netwerkomgeving te beschermen tegen steeds geraffineerdere bedreigingen.

Cisco Umbrella

Een cloudbeveiligingsservice die ingebouwde bescherming biedt voor uw internetservice

Cisco Umbrella is een cloudbeveiligingsservice die ingebouwde bescherming biedt tegen aanvallen via uw internetverbinding. Hierdoor hoeft u minder tijd en kosten te besteden aan het bestrijden van cyberaanvallen.

De oplossing biedt proactieve bescherming tegen bedreigingen op het internet, zoals malware, botnets en phishing-aanvallen. Uw bedrijf blijft beveiligd doordat verkeer wordt 'geschoond' voordat deze uw interne netwerk bereikt, de service leert waar aanvallen worden opgezet en bedreigingen op alle poorten en protocollen worden geblokkeerd. U kunt erop vertrouwen dat u dankzij beveiligde internettoegang met een eerste verdedigingslaag tegen malware beschermd bent.

Cisco Umbrella biedt zichtbaarheid van alle internetaanvragen op uw netwerk, op elke poort, via elk protocol en elke app om verbindingen met kwaadaardige domeinen en IP-adressen te detecteren en te blokkeren. Lees waarom kleine bedrijven het beveiligingsvermenigvuldigingseffect realiseren door DNS in te zetten als aanvulling op bestaande beveiligingsmaatregelen. Welke aanvallen ziet u niet?

Firewall van de volgende generatie

Een traditionele firewall regelt het verkeer op het ingangs- of uitgangspunt binnen het netwerk. De firewall vormt dus de ophaalbrug tussen uw eigen bedrijf en het 'ongeschoonde' deel van het internet.

Vroeger was dat voldoende, toen u nog kon zien wie of wat verbinding maakte met uw netwerk. Tegenwoordig zijn bedrijven steeds vaker host van talrijke onbekende apparaten en een enorme zee aan cloudtoepassingen die door werknemers worden gedownload.

Het grootste verschil met een firewall van de volgende generatie is dat u nu toepassingscontroles en -beleid kunt instellen. Als een teamlid bijvoorbeeld software voor bestandsdeling downloadt die mogelijk onbeveiligd is, wordt dat automatisch zichtbaar gemaakt en kunt u direct actie ondernemen.

Bovendien verkrijgt u veel meer zichtbaarheid en controle van gebruikers, apparaten, bedreigingen en kwetsbaarheden binnen uw netwerk. Wanneer uw directie u dan vraagt “Zijn we beveiligd?”, kunt u een uitgebreider antwoord geven dan als u een traditionele firewall gebruikt waarmee alleen het verkeer wordt geregeld.

Leer meer over firewalls van de volgende generatie of zoek de voor u beste firewall van de volgende generatie.

Advanced Malware Protection

Endpointbeveiliging van de volgende generatie

Endpointbeveiliging van de volgende generatie omvat de integratie van preventie-, detectie- en responsmogelijkheden in één oplossing, waarbij gebruik wordt gemaakt van de kracht van cloudgebaseerde analyses. Cisco AMP for Endpoints is een lichtgewicht connector die werkt op Windows-, Mac-, Linux-, Android- en iOS-apparaten.

Cisco AMP for Endpoints biedt uitgebreide bescherming tegen de meest geavanceerde aanvallen. De connector voorkomt inbreuken en blokkeert malware op het ingangspunt, en detecteert, beperkt en herstelt snel geavanceerde bedreigingen die de eerstelijns verdediging omzeilen en uw netwerk weten binnen te dringen.

Voorkomen: versterk de verdediging met de beste wereldwijde bedreigingsinformatie en blokkeer zowel ‘fileless’ (bestandsloze) als bestandsgebaseerde malware in real time.

Detecteren: bewaak en registreer alle bestandsactiviteit doorlopend om snel heimelijke malware te detecteren.

Reageren: versnel onderzoeken en herstel malware automatisch op pc’s, Macs, Linux-systemen, servers en mobiele apparaten (Android en iOS).

AMP kan gebruikmaken van de openbare cloud of als een private cloud worden geïmplementeerd. De bestands- en procesactiviteiten binnen uw netwerk worden doorlopend bewaakt en geanalyseerd om de 1% aan bedreigingen te detecteren die door andere oplossingen worden gemist. Via AMP wordt precies bijgehouden waar een bestand naartoe gaat of wat het doet. Als een bestand dat bij initiële inspectie als schoon wordt aangemerkt ooit kwaadaardig gedrag gaat vertonen, is in AMP de gehele geschiedenis van het gedrag van de bedreiging beschikbaar, zodat deze kan worden gedetecteerd, beperkt en opgelost.

Ontdek onbekende bedreigingen

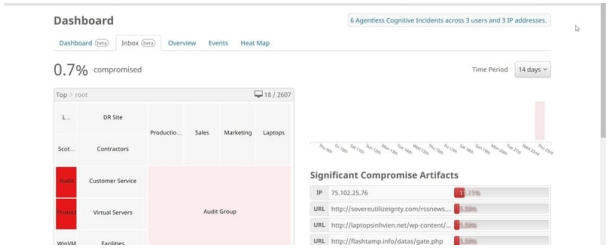
Met behulp van AMP's die in sandboxtechnologie zijn ingebouwd, wordt het gedrag van verdachte bestanden geanalyseerd en gecorreleerd met andere informatiebronnen. Bestandsanalyse produceert gedetailleerde informatie, zodat u beter weet hoe u de uitbraak kunt beperken en toekomstige aanvallen kunt blokkeren.

Wanneer een bestand als kwaadaardig wordt aangemerkt, kunt u met AMP de tijd en resources die nodig zijn voor een onderzoek aanzienlijk verminderen. AMP biedt automatisch inzicht rondom uw belangrijkste vragen, zoals:

- Wat is er gebeurd?
- Waar komt de malware vandaan?
- Waar is de malware geweest?
- Wat doe de malware nu?
- Hoe houden we de malware tegen?

Met enkele klikken in AMP's browsergebaseerde beheerconsole kunt u voorkomen dat het bestand wordt uitgevoerd op alle endpoints. Cisco AMP kent elk ander endpoint waar het bestand is geweest, waardoor het voor alle gebruikers in quarantaine kan worden geplaatst. AMP zorgt ervoor dat malware wordt uitgeroeid, zonder dat IT-systemen of het bedrijf schade wordt berokkend.

Een bestand tegenhouden en in quarantaine plaatsen met Cisco AMP:



Cisco Meraki

Cloudbeheerde beveiliging en SD-WAN

100% gecentraliseerd cloudbeheer voor beveiliging, netwerken en toepassingscontrole.

Cisco Meraki-beveiligingsapplicaties kunnen in enkele minuten op afstand worden geïmplementeerd met zero-touch cloudprovisioning. Beveiligingsinstellingen kunnen probleemloos op duizenden sites worden geconfigureerd met behulp van sjablonen. Met Auto VPN-technologie kunnen vestigingen met drie klikken op een beveiligde manier worden verbonden via een intuïtief, webgebaseerd dashboard.

Uitgebreide beveiliging in één pakket

Elke Meraki-beveiligingsapplicatie ondersteunt diverse functies, zoals een stateful firewall en geïntegreerde Sourcefire IPS-engine voor inbraakpreventie, om netwerken te beveiligen. Bedreigingsdefinities en filterlijsten worden naadloos bijgewerkt, zodat elke site profiteert van geavanceerde bescherming tegen de nieuwste kwetsbaarheden en problematische websites.

Beveilig een site in enkele minuten

1. Voeg de Meraki-beveiligingsapplicatie toe aan het dashboard.
2. Schakel inbraakpreventie in.
3. Selecteer het gewenste beschermingsniveau tegen bedreigingen.

Meer informatie

Ga voor de nieuwste inzichten en innovatie naar: Cisco Tech Connection for SMB of bekijk andere Cisco-resources voor MKB-bedrijven en Cisco-beveiligingsoplossingen om uw bedrijf te beschermen.

Hartelijk dank voor het lezen van

Essentiële beveiligingsinformatie voor MKB-bedrijven