ik wil mobiel werken

De security driehoek: policy, gebruiker en techniek

in samenwerking met

Wil je aan de slag met security? Dan krijg je altijd te maken met een samenspel van drie factoren: policy, gebruiker en technische oplossingen. Deze drie elementen zijn eigenlijk niet los van elkaar te zien. Ze hebben voortdurend invloed op elkaar. In deze longread lees je waar je per factor op moet letten, en welke stappen je als IT/security-manager moet nemen.

400%

Het aantal malware- en ransomware-incidenten is met 400% toegenomen

Hoe staat het met je beleid?

Voordat je aan de slag gaat met het verbeteren van je cybersecurity, is het belangrijk om in kaart te brengen waar binnen je organisatie knelpunten zitten. Pelle Aardewerk is cybersecurity expert bij HP, hij legt uit dat je moet starten met risicomanagement. “De wereld verandert razendsnel, er komen voortdurend nieuwe technologieën, en bijbehorende security risico’s bij. Daarom is het belangrijk om regelmatig even de temperatuur op te nemen op cybersecuritygebied.”

Bij zo’n risicoanalyse breng je je ‘cybersecurity maturity’ in kaart op basis van een risk-based assessment met betrekking tot bedreigingen, kwetsbaarheden en business impact. “Je kunt niet alles beschermen, hierin moet je keuzes maken op basis van een business case.” Welke gevoelige of persoonlijke data en bedrijfskritische systemen moet je hoe dan ook beschermen tegen cybercriminelen? Met welke bedreigingen kun je hierbij te maken krijgen? Vervolgens bepaal je hoeveel risico je loopt op welk gebied. Hiervoor vermenigvuldig je de waarschijnlijkheid dat je te maken krijgt met een cyberaanval, met de impact.

Welke policies en standaarden heb je nodig?

Wist je dat er ruim 30 verschillende policies en standaarden zijn op het gebied van cybersecurity? Pelle licht de belangrijkste zeven uit:

01 Acces Management

Identificatie en toegang per eindgebruiker tot bepaalde documenten en systemen op basis van zijn of haar rol met behulp van multifactorauthenticatie.

02 Endpoint security

Hoe beveilig je de endpoints (waar de gebruiker, het internet, apps en data samenkomen) tegen sterk toenemende cyber security aanvallen? Tevens; is er een actueel veilig hybride werken beleid?

03 Cloud infra security

Hoe zorg je ervoor dat er veilig in de cloud gewerkt kan worden met derde partijen? En hoe krijg je via de cloud veilig toegang tot je apps en data?

04 Data security

Hoe bescherm je de belangrijkste data van het bedrijf, en de data van je klanten? Hoe zorg je daarnaast voor GDPR-compliance?

05 Netwerk security

Hoe beveilig je zero-trust based netwerken en communicatie hiertussen?

06 Applicatie security

Hoe bepaal je welke applicaties je medewerkers mogen gebruiken, en toegang hiertoe?

07 Incident and response management

Wat doe je als het mis gaat, en er toch een cyberaanval plaatsvindt om zo snel mogelijk weer up- and running te kunnen zijn met minimale impact?

'De wereld verandert razendsnel, er komen voortdurend nieuwe technologieën, en bijbehorende security risico's bij.'

Pelle legt uit dat het bij veel bedrijven in geval van crisis onduidelijk is wie er verantwoordelijk is voor cybersecurity. “Als er iets gebeurt, heb je iemand nodig die opstaat en crisismanagement gaat leiden. Houd er ook rekening mee dat de baan van Chief Information Security Officer (CISO) erg zwaar is. Je bent cyber security evangelist, eindverantwoordelijke en expert in een snel veranderende omgeving. Je hebt tegelijkertijd niet altijd de buy-in, funding en resources die je nodig hebt om je securitystrategie tijdig te bewerkstelligen.

Securitychecklist policies

☑ Breng met behulp van risicomanagement periodiek in kaart waar je prioriteiten liggen en update je cybersecuritystrategie/roadmap.

☑ Zorg dat je de belangrijkste risk-based security policies hebt geïmplementeerd (qua begrip en operationalisatie) binnen je organisatie en in samenspraak met je IT partners en suppliers.

☑ Wijs binnen je organisatie verantwoordelijke aan wanneer er een cyberaanval plaatsvindt en oefen dit scenario.

De mens als zwakke schakel

Al is je beleid nog zo goed geschreven, wanneer medewerkers hier niet mee aan de slag gaan, heb je een probleem. Eindgebruikers zijn volgens Pelle vaak een zwakke schakel op het gebied van cybersecurity. “We zien dat mensen door verbeterde technologie hybride en steeds productiever kunnen werken, maar hierdoor veel onveilig gedrag vertonen. Zo gaan ze tijdens het thuiswerken op de werklaptop bijvoorbeeld privédingen doen. Of ze klikken op allerlei linkjes en downloaden onveilige bestanden. Dat zijn grote risicofactoren voor toenemende security-incidenten, want ondanks geïmplementeerde oplossingen zoals Next-Generation Antivirus en Endpoint detection and response is het aantal malware- en ransomware-incidenten is met 400% toegenomen.”

Volgens Pelle is het goed mogelijk om medewerkers bewust te maken van hoe ze op een veilige manier kunnen werken. “Je kunt mensen hier op trainen”, vertelt hij. “Focus hierbij niet alleen op de gebruikers binnen je eigen bedrijf, maar kijk ook of je andere partijen binnen je IT-ecosysteem en supply chain kunt trainen. We verwachten namelijk dat er steeds meer aanvallen binnen supply chains zullen plaatsvinden.”

Na de training kun je medewerkers scherp houden door regelmatig updates te sturen over cybersecurity op een praktische en leuke manier (zoals security games). Ook is het een goed idee om met behulp van nep-phishingmailtjes medewerkers te verleiden op een link te drukken of een document te downloaden. Als je vervolgens aangeeft dat ze in de handen van een nep-hacker zijn beland, begrijpen ze hoe urgent het probleem is en is het aan te raden ze een specifieke training te laten volgen. Pelle benadrukt hierbij dat het wel belangrijk is om een balans te vinden. “Wanneer je te veel aandacht besteedt aan het onderwerp, kunnen mensen vermoeid raken en de informatie niet meer opnemen.”

Securitychecklist gebruiker

☑ Maak medewerkers, leveranciers en klanten (verder) bewust van de risico’s met een training over cybersecurity. Hier leg je uit wat gewenst gedrag is.

☑ Verstuur een nieuwsbrief tips en tricks op het gebied van IT en security, bijvoorbeeld voor veiliger hybride werken.

☑ Controleer of je medewerkers scherp zijn op dreigingen met behulp van een nep-phishingmailtje, opgevolgd met een compliment of een toepasselijke training.

De juiste techniek

Technologische innovatieve ontwikkelingen volgen elkaar in rap tempo op. De manier waarop we werken zal ingrijpend blijven veranderen met steeds betere functionaliteit en toegang tot apps en data. Daarom is het slim om regelmatig

security- en privacy-assessments uit te voeren en implicaties te doorgronden voordat je een nieuwe technologie in huis haalt. Hierdoor kun je technologische verandering op een *secure by design* wijze implementeren en je security oplossingen financieren in het project.

Voor IT- en cybersecuritymanagers kan het lastig zijn om nieuwe vormen van cybercrime buiten de deur te houden. Een securitybeleid en veilig gedrag van medewerkers is niet voldoende, het is essentieel om technische security-oplossingen te implementeren. Met deze factoren samen verklein je het risico op een cyberaanval. Pelle legt uit dat het belangrijk is voor elke policy uit het vorige hoofdstuk passende technische oplossingen te zoeken. Deze moeten (liefst geïntegreerd) op een overzichtelijke manier beveiliging en zichtbaarheid opleveren. Dat kan via een Security Incident and Event Management (SIEM) systeem voor je 24/7 Security Operation Center (SOC).” Veel bedrijven kunnen dit niet zelf en besteden dit uit op basis van ‘security as a service’.

De zero trust endpoint security

Ken je de zero trust filosofie al? Deze manier van werken draait om het feit dat je op IT-gebied niks vertrouwt en alles te allen tijde verifieert. Mede door digitalisatie, cloud transformatie en hybride werken vindt er op het gebied van security een transformatie plaats van ‘zero- trust network perimiter security’ naar ‘endpoint security’. Zowel applicaties, data, devices als gebruikers werken nu productiever buiten het beveiligde bedrijfsnetwerk. “Hierdoor zien we dat meer dan 70% van de aanvallen zich richt op medewerkers die klikken op onveilige bestanden en browsers via hun device (waar het internet, apps, data en de gebruiker samenkomen). We verwachten daarom in de komende jaren exponentiële groei op endpointsecurity-gebied.”

Pelle legt uit dat vanuit deze focus op endpoints zowel de gebruiker als het device en inkomende data moeten worden onderworpen aan controles. Zo moet de gebruiker aan de slag met multifactor authenticatie. Dat is veiliger dan het gebruik van wachtwoorden, die kunnen namelijk worden gestolen. Devices kunnen worden beveiligd met behulp van securitytools als het HP Wolf Security Platform Portfolio.

Hoe ziet zo'n zero trust endpoint securityoplossing er dan uit?

Verifieer de identiteit en toegang van de gebruiker:
Dit kan met behulp van identity- en access-management via multifactorauthenticatie. Toegang tot bepaalde data, applicaties en documenten is hierbij ingeregeld gebaseerd op informatie over de gebruiker en het device.

Verifieer de integriteit van laptops en printers:
"Gebruik een secure platform zowel boven, in als onder het operating system.", adviseert Pelle. "De HP Wolf Secure Platform oplossingen zorgen voor de beste beveiliging tegen onder andere firmware-, malware- en ransomware-aanvallen." Deze tools waarborgen de integriteit van de computersystemen. Een voorbeeld is HP Wolf Sure Start. Deze oplossing komt in actie als het BIOS van een device wordt aangevallen. De bedreiging wordt door middel van deep learning-algoritmen en neural network technology direct herkend. Vervolgens wordt het apparaat automatisch opnieuw opgestart en wordt een 'gouden kopie' van de BIOS geladen.

Verifieer veilig klikken op onbetrouwbare bestanden en browsers:
Naast detectieoplossingen als Next-Generation Antivirus en Endpoint detection and response, Is het belangrijk om isolatietechnologie in te zetten. Een voorbeeld van zo'n technologie is Wolf Secure Click Enterprise. Hiermee kunnen medewerkers veilig klikken op bestanden en websites. Het bestand of de pagina in kwestie wordt namelijk in een soort veilige 'container' geplaatst waaruit de malware niet kan ontsnappen. Een ander voorbeeld is HP Wolf Sure Access Enterprise. Hiermee kun je veilige remote admin sessies met geprivilegieerde gebruikerstoegang garanderen.

Verifieer de laptop locatie, eigenaar en veilig gebruik op afstand in geval van verdwenen laptops:

Pelle vertelt uit dat één op de tien laptops ooit zoek raakt tijdens de levenscyclus. "Met behulp van HP Wolf Protect & Trace kun je laptops op afstand traceren, versleutelen en gevoelige data verwijderen." In dit filmpje zie je hoe het Protect & Trace-principe werkt.

Securitychecklist techniek

☑ Maak een security risicoanalyse bij nieuwe technologieën en pas het security by design-principe toe tijdens het project.

☑ Gebruik een alles-in-een securityoplossing zoals HP Wolf Platform Security (standaard inbegrepen en ingeschakeld bij HP laptops).

☑ Overweeg Security as a service.

☑ Focus op Zero Trust Endpoint Security. Gebruik HP Wolf isolatie technologie om de toenemende endpoint security aanvallen te voorkomen. Benieuwd hoe deze praktisch werken? Bekijk deze korte Sure Click Enterprise en Sure Access Enterprise video's.