MSP-PROGRAMMA

6 TIPS OM JOUW MSP-AANBOD ONWEERSTAANBAAR TE MAKEN

Als MSP'er moet je security-expertise tonen, een volledig portfolio aan beveiligingsoplossingen en -diensten bieden en toegevoegde waarde leveren aan jouw klanten.

1 Ken je klant

Een goed zakelijk partnerschap is gebaseerd op vertrouwen. Om een positieve toon te zetten, kun je overwegen een eerste veiligheidsaudit van de IT-systemen van jouw klant uit te voeren. Dit zal jouw deskundigheid demonstreren en de informatie over bedreigingen genereren die nodig is om de huidige beveiligingsstrategie van de klant aan te passen – of om vanaf nul een nieuwe strategie te creëren.

De lijst hiernaast is niet uitputtend, maar de uitkomsten ervan kunnen de verschillende behoeften die zich in verschillende sectoren voordoen duidelijk maken. In de landbouw kan IT worden gezien als een "noodzakelijk kwaad" dat alleen maar hoeft te werken. Een klant die actief is in de gezondheidszorg zal daarentegen waarschijnlijk een bedrijfsmodel hebben dat gebaseerd is op het verzamelen en analyseren van gevoelige patiëntinformatie, dus zijn gegevensversleuteling of andere technologieën gericht op gegevensbescherming essentieel.

Dankzij dit eerste onderzoek kun je ook het dreigingsmodel identificeren dat op jouw klant van toepassing is en hen als onderdeel van de diensten die je levert **voorzien van een beveiligingspakket op maat** dat het beschermingsniveau zal verbeteren.

Een veiligheidsaudit moet onder andere antwoord geven op een aantal fundamentele vragen:

1. In welke sector is de klant actief en wat zijn de kenmerken van die sector?
2. Hoe en waarom gebruikt de klant zijn IT-systemen?
3. Wat wordt er opgeslagen op die systemen?
4. Worden de apparaten van de klant alleen op locatie of ook op afstand gebruikt?
5. Welke soorten gebruikers loggen in op het netwerk?
6. Welke IT-problemen heeft de klant in het verleden ondervonden?

2 Pas cyberhygiëne toe

Als software- en beveiligingsleverancier moeten jouw eigen systemen een voorbeeld zijn voor jouw klanten. Volg de beste cyberhygiënepraktijken voor jouw eigen systemen en pas deze vervolgens ook toe op de technische infrastructuur van je klanten. Door de inzet van goed patchbeheer en het up-to-date houden van besturingssystemen, apps en beveiligingsoplossingen kun je veel potentiële kwetsbaarheden verhelpen.

Je kunt **aanvalsoppervlakken verminderen** en het ontstaan van nieuwe gaten in de cyberbeveiliging voorkomen door de **toegangsrechten van jouw klant goed te beheren** bij het installeren van nieuwe software. Ook als de klant het onderhouden van hun software en beveiligingsoplossingen door de interne IT-afdeling wil laten uitvoeren, moet een soortgelijke aanpak worden aangeraden.

Het belang van cyberhygiëne werd benadrukt door het Wanna-Cryptor.D (ook wel WannaCry) incident in 2017. Ondanks dat de kwetsbaarheid in Windows al maanden voor de aanval **bekend was en gepatcht werd**, hadden honderdduizenden endpoints de update niet doorgevoerd, waarvan een groot deel in het mkb-segment.

Schoon jouw IT-praktijken op

1. Verminder het aanvalsoppervlak door onnodige diensten en software uit te schakelen of te de-installeren
2. Scan netwerken op risicovolle accounts die gebruikmaken van zwakke wachtwoorden en zorg ervoor dat deze worden verbeterd
3. Beperk of verbied het gebruik van Remote Desktop Protocol (RDP) van buiten het netwerk, of schakel authenticatie op netwerkniveau in
4. Gebruik een VPN voor toegang op afstand
5. Bekijk de instellingen van de firewall en sluit alle niet-essentiële poorten
6. Beoordeel het huidige beleid voor verkeer tussen interne bedrijfssystemen en externe netwerken
7. Bescherm de configuraties van beveiligingsoplossingen met een wachtwoord
8. Segmenteer het LAN van het bedrijf in subnetten en sluit deze aan op firewalls om de potentiële impact van aanvallen binnen het netwerk te beperken
9. Bescherm back-ups met multifactorauthenticatie
10. Train medewerkers in het herkennen van cyber- en social engineering-aanvallen
11. Beperk de toegang tot gedeelde bestanden/mappen tot alleen degenen die het nodig hebben, en maak de inhoud waar mogelijk alleen-lezen
12. Schakel detectie van potentieel onveilige/ongewenste applicaties (PUSA/PUA) in

3 Kies de juiste beveiligingsoplossingen

Het opnemen van endpointbeveiliging en beveiligingsmiddelen zoals een firewall en antispam in jouw aanbod is essentieel. Maar het aanbieden van aanvullende oplossingen — gebaseerd op de behoeften van jouw klanten en de juridische vereisten van de sectoren waarin zij opereren — kan je een voorsprong geven. Denk hierbij aan dataversleuteling, een cloud sandbox, multifactorauthenticatie of data loss prevention (DLP).

Al deze **oplossingen moeten onderhoudsarm, eenvoudig te implementeren en makkelijk in het gebruik zijn**, omdat je daardoor jouw capaciteiten kunt inzetten waar het nodig is en de klant in staat stelt om ongestoord te werken. ESET-oplossingen zijn ontworpen om aan jouw behoeften (en die van jouw klanten) te voldoen door te werken volgens het "installeer en vergeet"-principe. Om van hun volledige potentieel te profiteren, volgen hier enkele basisregels waar gebruikers zich aan zouden moeten houden:

- **Gebruik de nieuwste versie** van elk product
- **Houd beveiligingsfuncties** zoals ESET LiveGrid® en realtime-scanning **ingeschakeld**. Deze systemen zijn ontworpen om informatie over bedreigingen te verzamelen en het beschermingsniveau van de gebruikers te verhogen
- **Update**, als de internetverbinding het toestaat, **altijd de scanning engine en de detectiedatabase** om ervoor te zorgen dat beheerde werkstations worden beschermd tegen nieuwe en opkomende bedreigingen
- **Voer geen handmatige scans uit**, omdat dit hardwarevermogen verbruikt voor onnodige herhaling van de activiteiten van de realtime scans

Klik hier om meer te leren over ESETs diensten voor Managed Service Providers.

ESET raadt niet aan dat gebruikers zelf scans uitvoeren, met uitzondering van de eerste scan na installatie. Daarna zorgt **realtime beveiliging** voor alle nieuwe items die eventueel opduiken op het systeem. De enige keer dat gebruikers zelf een scan moet uitvoeren, is nadat realtime-bescherming handmatig uitgeschakeld is geweest.

4 Train jouw klanten en hun gebruikers

Als externe beveiligingsadviseur kun je ook toegevoegde waarde leveren door de medewerkers van jouw klanten cybersecuritytraining en -educatie te bieden. Dit moet worden afgestemd op het niveau van de technische kennis van de medewerkers, met verschillende trainingen voor management, IT-personeel en reguliere gebruikers.

Reguliere gebruikers zijn de eerste verdedigingslinie tegen cyberdreigingen binnen een organisatie. Zij kunnen aanvallen voorkomen als zij weten hoe ze om moeten gaan met eenvoudige social engineering-technieken, phishing en andere cyberaanvallen. Daarom moet hun training zo breed mogelijk zijn, te beginnen bij de basis:

- Beschrijving van de meest voorkomende dreigingen zoals malware, social engineering en phishing
- Regels voor goede wachtwoordhygiëne en het belang van multifactorauthenticatie
- Best practices voor het verbinden met netwerken
- Tips en regels voor veilig browsen
- Uitleg over spearphishing, whalephishing en gerichte campagnes van cybercriminelen – met name voor het management en medewerkers die met gevoelige data werken

MSP'ers zouden daarnaast ook een speciaal programma moeten hebben voor de IT-medewerkers van hun klanten, met bruikbare tips en best practices voor het inrichten van de beveiligingsoplossingen, netwerken en systemen. Vergeleken met trainingen voor het management of de eindgebruikers, moeten de programma's voor IT-personeel dieper ingaan op de techniek en een breed scala aan onderwerpen behandelen:

- Minimale wachtwoordvereisten, frequentie en opzet van een wachtwoordbeleid
- Correcte setup van admin- en gebruikersprofielen op het bedrijfsnetwerk
- Tips voor het minimaliseren van het aanvalsoppervlak van interne systemen
- Specifieke instellingen voor legitieme diensten die vaak worden misbruikt als aanvalsvectoren, zoals het Remote Desktop Protocol (RDP), of e-mails en e-mailbijlagen
- Gedetailleerd advies voor het voorkomen van ransomware

ESET biedt lesmaterialen, gidsen en tips voor MSP-partners, gemaakt om te delen met jouw klanten

5 Zet een goede infrastructuur op en ga in gesprek met de klant

Communicatie is belangrijk, maar soms geldt: less is more. Klanten verwachten dat je hen in duidelijke en begrijpelijke taal informeert over wat er in hun IT-systemen gebeurt – maar alleen wanneer dat nodig is. Te veel meldingen over kleine gebeurtenissen kunnen hinderlijk worden voor de klant en het vertrouwen in jouw capaciteiten aantasten.

Een MSP'er moet gebruik maken van beveiligingstools die gedetailleerde informatie verschaffen en een overzicht geven van afwijkingen op werkstations of andere onderdelen van het systeem die mogelijk aandacht nodig hebben.

In het geval van een veiligheidsincident moet een MSP'er beschikbaar zijn en de middelen hebben om **snel te reageren** en problemen die het incident kan veroorzaken op te lossen. Indien mogelijk dient de situatie **op afstand** te worden behandeld en opgelost. Om dit doel te bereiken zijn een goed geschaalde en **zeer flexibele infrastructuur** en **betrouwbare netwerkverbindingen** nodig.

Als MSP'er moet je ook **in staat zijn om jouw systemen, infrastructuur en software te schalen en aan te passen** aan de voortdurend veranderende behoeften van jouw klanten.

ESET biedt een krachtige, multi-tenant beheerconsole: **ESET PROTECT**. Hiermee heb je een dynamisch, real-time overzicht van potentiële dreigingen die een risico vormen voor de bedrijfscontinuïteit van jouw klanten. Deze gebruiksvriendelijke oplossing geeft je de mogelijkheid de afhandeling van beveiligingsproblemen te automatiseren en aanpasbare rapportages te genereren met jouw logo, die je naar jouw klanten kunt sturen.

6 Vermijd het break/fix-model, wordt een moderne MSP'er

Het aanbieden van IT-beveiligingsdiensten volgens het oude "break/fix"-model behoort steeds meer tot het verleden. Jouw klanten willen tijdrovende – en prijzige – reparaties op locatie vermijden, en hetzelfde geldt voor het moeten signaleren van problemen en het onderhouden van hun eigen systemen.

Overweeg als moderne MSP'er jouw klanten het volgende aan te bieden:

- **Diensten met toegevoegde waarde:** Het gaat niet meer om het verkopen van producten. Een moderne MSP'er moet waarde op de tafel leggen en klanten overtuigen dat het de moeite waard is om in deze diensten te investeren in plaats van in het opbouwen van interne capaciteiten.
- **Reguliere monitoring:** In plaats van alleen maar te installeren en de controle over de IT en beveiliging vervolgens over te dragen aan de klant, biedt een moderne MSP'er constante monitoring en onderhoud van de oplossingen die zij bieden. Dit neemt een last weg aan de klantzijde en stelt de MSP'er in staat om voortdurend op de hoogte te blijven van zowel de stand van zaken als de veranderingen in de systemen en netwerken van hun klant.
- **Open en maandelijkse facturering:** Net als bij veel andere online diensten hebben MSP'ers het model van open en maandelijkse facturering aangenomen. Dit biedt klanten meer flexibiliteit en snel inzetbare diensten en oplossingen.
- **Regelmatig overleg met klanten:** In tegenstelling tot het vroegere model moeten moderne MSP'ers regelmatig communiceren met klanten. Dit creëert sterkere relaties en helpt misverstanden te voorkomen.
- **Problemen oplossen op afstand:** Een handige, minder tijdrovende en bovenal snellere manier om problemen op te lossen vergeleken met het oude op locatie-model.

Klanten moeten altijd **een eenvoudige manier hebben om contact met je op te nemen**. Als je er zeker van wilt zijn dat dit duidelijk gecommuniceerd is, maak dan bureaubladachtergrond aan waar de contactgegevens van jouw bedrijf in zijn verwerkt. Dit maakt jouw supportteam bereikbaar en toegankelijk in geval van IT-noodgevallen.

6 TIPS OM JOUW MSP-AANBOD ONWEERSTAANBAAR TE MAKEN

Als MSP'er moet je security-expertise tonen, een volledig portfolio aan beveiligingsoplossingen en -diensten bieden en toegevoegde waarde leveren aan uw klanten.

ESET Nederland
Trapezium 304, 3364 DL Sliedrecht

Ashley Schut
Solution Advisor MSP
ashley.schut@eset.nl
+31 (0)6 11 14 45 69
+31 (0)184 647 740

www.eset.com/nl

CYBERSECURITY
EXPERTS ON YOUR SIDE