Hoe je een effectieve cybersecurity-strategie opstelt

Een gids voor kleine- en middelgrote organisaties

Digital Security
Progress. Protected.

In grote bedrijven zijn er meestal complete afdelingen die toezicht houden op de cyberveiligheid van het bedrijf en effectieve strategieën opzetten. Maar hoe zit het met kleine en middelgrote bedrijven (mkb), met slechts een paar interne IT-specialisten? Hoe moeten zij te werk gaan om ervoor te zorgen dat het bedrijf op de juiste manier wordt beschermd, zonder overweldigd te raken door alle mogelijke maatregelen?

Hier zijn een paar tips van **Michal Jankech, vicepresident van het SMB & MSP segment bij ESET**.

Digital Security
Progress. Protected.

Waar te beginnen?

In de meeste gevallen hebben mkb-bedrijven weinig of geen personeel dat zich bezighoudt met digitale beveiliging. Daarom is het cruciaal dat ze zich richten op de grootste dreigingen en hun energie steken in zaken die essentieel zijn voor hun bedrijfscontinuïteit.

"**Ze moeten een op risico gebaseerde aanpak hanteren waarbij de meest cruciale kwatsbaarheden worden geïdentificeerd,**" aldus Jankech, die hieraan toevoegt dat MKB's eerst de beveiligingsgebieden moeten aanpakken die hiernaast genoemd worden.

- **Gegevensbescherming en encryptie**
- **Meerlaagse bescherming voor endpoints en toegangsbeperkingen voor gebruikers**
- **MFA* en regelmatige updates**
- **Hoogwaardige e-mailproviders en opleiding van werknemers**
- **EDR* of MDR* voor organisaties die diepgaand inzicht in hun bedrijfsnetwerk nodig hebben niveaus**

***Multifactorauthenticatie/Endpoint Detection & Response/Managed Detection & Response**

Gegevensbescherming en encryptie

Zijn al je apparaten vergrendeld met een gebruikersnaam en een sterk wachtwoord? Dan is dat een goede eerste stap, maar toch is er meer wat je moet doen als je je apparaten zo goed mogelijk wilt beveiligen.

“**Alle endpoints zouden gebruik moeten maken van encryptie**. Stel je voor dat iemand je computer steelt, dan kunnen ze dus niet inloggen omdat ze de gebruikersnaam en het wachtwoord niet weten. Maar toch kunnen ze toegang krijgen tot de gegevens door de harde schijf eruit te halen. Het is dus belangrijk om ervoor te zorgen dat niet alleen draagbare apparaten encryptie bevatten, maar ook desktop computers”, adviseert Jankech.

“Ik heb ooit een gezondheidsinstelling bezocht en zag daar dat ze een computer hadden bij de kiosk. Deze computer was niet beveiligd met een wachtwoord waardoor iemand gemakkelijk de pc kon stelen, om zo toegang te krijgen tot gegevens van de patiënten. Soortgelijke scenario’s kunnen worden voorkomen door effectieve gegevensbescherming en encryptie-maatregelen”

Meerlaagse bescherming voor endpoints en toegangsbeperkingen voor gebruikers

“Het is cruciaal om admin gebruikersaccounts te beperken. In veel gevallen zijn het mensen die veel schade kunnen aanrichten. Als kwaadwillenden toegang krijgen tot het beheerdersaccount, kunnen ze potentieel alles op het apparaat installeren”, aldus Jankech.

Realiseer je ook dat één beschermingslaag niet voldoende is. “Het is als het beveiligen van een gezinswoning. In dat geval zou je ook maatregelen nemen die je verdediging versterken - deuren met goede sloten, ramen die dichtgedaan worden, een hek en misschien zelfs wel een alarm en/of beveiligingscamera’s. Veel mensen zeggen dat de tijd van antivirus voorbij is. Ja, de tijd van standaard antivirus, die alleen werkt op dezelfde manieren, is voorbij. Deze oplossingen zijn niet in staat om ons effectief tegenover huidige dreigingen te verdedigen”, vervolgt Jankech.

In plaats daarvan, wordt software voor **meerlaagse bescherming voor endpoints**, die gebaseerd is op

> **Voor MKB’s is het zinvol om te investeren in preventie. Het versterken van jouw systemen, ze up-to-date houden en het gebruik van goede software voor de bescherming van endpoints is van belang.**
>
> **Michal Jankech**,
> VP van het SMB & MSP segment bij ESET

de principes van machine learning en die bescherming biedt op basis van gedrag, aanbevolen. Waarbij onveilige websites op een blacklist worden gezet en de toegang tot riskante domeinen, inclusief bescherming tegen netwerk aanvallen of kwetsbaarheden in het desktop protocol die misbruikt kan worden.

“Het gaat er niet alleen om dat je bescherming hebt, maar ook de juiste configuratie en updates” voegt Jankech toe. Bijvoorbeeld, ervoor zorgen dat de software voor de bescherming van endpoints niet kan worden verwijderd, of de configuratie ervan kan worden gewijzigd, is van belang.

Gebruik vervolgens een **beheerconsole voor endpoints**. “Veel bedrijven denken dat het voldoende is om een endpoint beschermingsclient te gebruiken. Maar je weet nooit of het goed werkt als je het niet beheert via een console waarmee je het hele netwerk kunt overzien. Zelfs als je slechts 10 computers in het bedrijf hebt, is het lastig om ze goed te controleren. Vooral tegenwoordig, wanneer mensen steeds meer thuiswerken en reizen,” zegt Jankech. Tegelijkertijd moet de console jou voorzien van rapporten die je kunt controleren om er 100% zeker van te zijn dat jouw systemen en netwerkverkeer in ideale staat zijn.

MFA en regelmatige updates

Multifactorauthenticatie (MFA) moet aanwezig zijn op alle werk- en privéapparaten. Ook is het belangrijk dat alle systemen op hun laatste versie draaien. “De meeste inbreuken ontstaan door identiteits- en wachtwoorddiefstal of een algemeen bekende kwetsbaarheid in het besturingssysteem die kan worden misbruikt”, legt Jankech uit.

Bij elke nieuwe versie van het besturingssysteem herstelt de vendor de mogelijke gaten, en verklein je de kans dat cybcercriminelen de weg kunnen vinden naar bedrijfsapparaten. **Automatische updates worden aanbevolen.** “Wanneer het gaat om het MKB, komen zero day-aanvallen zelden voor. Als je speciaal gebouwde software gebruikt, is de kans dat cybercriminelen zo’n gerichte aanval uitvoeren vrij laag. In de meeste gevallen zijn wijdverspreide kwetsbaarheden in algemeen gebruikte of open-source software de manier waarop aanvallers jouw bedrijf binnenkomen”, zegt Jankech.

> **“Artsen, architecten, PR-bureaus… allemaal hebben ze een cyberbeveiligingsstrategie nodig. Veel mensen weten bijvoorbeeld niet dat bepaalde documenten beschermd zijn door auteursrecht en dus op de juiste manier moeten worden beschermd.”**
>
> **Michal Jankech**,
> VP van het SMB & MSP segment bij ESET

Hoogwaardige e-mailproviders en opleiding van werknemers

Ook betrouwbare e-mailproviders zijn belangrijk. “Ook moeten werknemers weten hoe ze een phishing e-mail kunnen detecteren. Je kunt ook elke ontvanger laten weten dat het bericht afkomstig is van buiten het bedrijf. Zelfs met Office 365 kun je e-mails als ‘extern’ labelen”, raadt Jankech aan. Van tijd tot tijd is het de moeite waard om te investeren in cybersecuritytraining van medewerkers om het bewustzijn te vergroten. **Je kunt tips lezen** over hoe je scholing effectief en leuk kunt maken op onze ESET Digital Security Guide.

Jankech benadrukt dat de meeste bedrijven deze basismaatregelen niet hebben, en dat er soms nog grotere gaten zitten in de digitale beveiliging van grote bedrijven. “Sommige bedrijven aarzelen nog steeds om te investeren in cybersecurity-oplossingen of denken dat ze geen doelwit kunnen worden, omdat hun branche hier niet voor in aanmerking zou komen bij dreigingsactoren. Maar meestal zijn cyberaanvallen niet gericht. Iedereen kan het slachtoffer worden.”

EDR of MDR voor diepgaand inzicht

Zodra je alle basisbenodigdheden voor cybersecurity hebt, is het tijd om **geavanceerde cybersecurity tools te overwegen- zoals Extended Detectie & Response (XDR)**. “Het is een geheel nieuwe manier van verdedigen, gebouwd op de vooronderstelling dat preventie altijd faalt. Dit deel van de productsuite is vooral van toepassing op grote ondernemingen die zich de luxe kunnen veroorloven van talrijke interne IT-afdelingen en een in-house SOC (Security Operations Center) met 24/7 werkzaamheden. Volgens deze aanpak betekent meestal dat je het standpunt inneemt dat cybercriminelen uiteindelijk met succes jouw systeem zullen aanvallen”, zegt Jankech.

De XDR-oplossingen identificeren onregelmatigheden en verdacht gedrag in het netwerk en laten je idealiter reageren door het proces te blokkeren - of de systemen handelen deze taken af via aangepaste geautomatiseerde regels. “Hoewel ze meestal worden gebruikt in grotere bedrijven, kunnen ze ook nuttig zijn voor kleinere bedrijven.

Essentiele bouwstenen in een cybersecuritystrategie voor het mkb

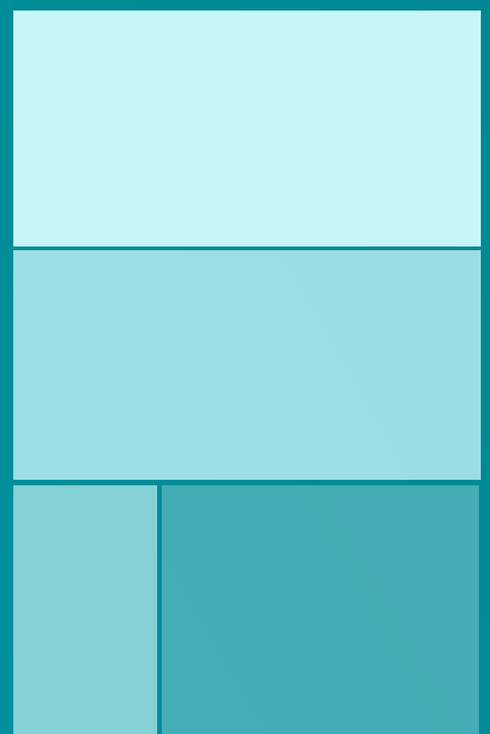
- **Beschermde en versleutelde gegevens**
- **Beperkte toegangsregels voor gebruikers**
- **Meerlaagse bescherming voor endpoints**
- **MFA en updates van het besturings-systeem**

Hoe dan ook, aangezien je personeel nodig hebt om jouw EDR platform te managen, is het aanbevolen dat kleinere bedrijven met een gebruikersscenario kijken naar het uitbesteden van dergelijke diensten," voegt Jankech toe.

Dit is waar zogenaamde MDR – Managed Detection en Response – komt kijken. MDR is XDR dat wordt beheerd door een derde partij. Ook kan MDR uitgevoerd worden, zonder dat er van een XDR-tool gebruikgemaakt wordt. "Vanuit 1 beheercentrum worden tientallen of zelfs honderden klanten bewaakt, en er is meestal een 24/7 hotline waar je ook terecht kunt," zegt Jankech.

Toch moet EDR of MDR alleen worden overwogen als je de basis al onder controle hebt. Als je er klaar voor bent, vergroot het gebruik van EDR of MDR de kans dat jouw bedrijf eventuele cyberaanvallen kan weerstaan, waarbij jouw bedrijf veilig maar altijd alert is.

Gebruik van EDR-/ XDR-/ MDR-oplossingen



33%
Is van plan om het binnen 12 maanden te gebruiken

32%
Gebruikt het momenteel

11%
Overweegt om het in de komende 2 jaar te gebruiken.

Bron: 2022 ESET SMB Digital Security Sentiment Report

OVER ESET

Al meer dan 3 decennia ontwikkelt ESET® toonaangevende IT-beveiligingssoftware en -diensten om bedrijven, kritieke infrastructuur en consumenten wereldwijd te beschermen tegen steeds complexere digitale bedreigingen. Inmiddels is ESET uitgegroeid tot het grootste IT-security bedrijf uit de Europese Unie met oplossingen variërend van endpoint en mobile security, tot encryptie en tweefactorauthenticatie. ESET beschermt en monitort 24/7 op de achtergrond en werkt beveiliging in real-time bij om gebruikers veilig te houden en bedrijven zonder onderbreking te laten werken. Evoluerende bedreigingen vereisen een evoluerend IT-beveiligingsbedrijf dat veilig gebruik van technologie mogelijk maakt. Dit wordt ondersteund door ESETs R&D centra wereldwijd, die zich inzetten voor onze gezamenlijke toekomst. Ga voor meer informatie naar www.eset.com/nl of volg ons op LinkedIn, Facebook, Instagram en Twitter.

Digital Security
Progress. Protected.