NEXT STEP 24 >

12 cybersecurity-aanbevelingen voor organisaties in 2026

Het dreigingslandschap zich ontwikkelen. Aanvallers maken gebruik van zowel traditionele als moderne technieken in hybride omgevingen. Deze 12 aanbevelingen helpen organisaties risico's te verminderen en hun weerbaarheid te vergroten, terwijl zij flexibel blijven om zich aan te passen aan veranderende dreigingen.

1. Minimaliseer blootstelling aan het internet

Organisatorische veranderingen zoals groei, fusies en overnames, transformatie-initiatieven of andere ontwikkelingen kunnen ervoor zorgen dat netwerkperimeters vervuild raken met verouderde of redundante systemen. Dit creëert gemakkelijke toegangspunten voor aanvallers.

- Verwijder ongebruikte systemen: Ruim tijdelijke, dubbele of end-of-life infrastructuur op.
- Schakel onnodige services uit: Deactiveer legacy-protocollen, ongebruikte VPN-typen en functionaliteiten die niet essentieel zijn voor de bedrijfsvoering.

2. Geef prioriteit aan patching en kwetsbaarheidsbeheer

Edge-apparaten zoals firewalls en VPN-systemen zijn aantrekkelijke doelwitten vanwege hun hoge toegangsrechten en beperkte zichtbaarheid.

- Patch actief misbruikte kwetsbaarheden: Focus op kwetsbaarheden die daadwerkelijk worden gebruikt in aanvallen. Voor de meeste zijn al patches beschikbaar.
- Houd een volledig assetoverzicht bij: Goede zichtbaarheid is essentieel voor het prioriteren van patches en het verminderen van risico's.
- Beveilig beheerinterfaces: Zorg dat deze niet publiek toegankelijk zijn en correct geconfigureerd zijn.
- Volg beveiligingsadviezen: Gebruik leveranciersupdates en bijvoorbeeld de KEV-catalogus van CISA om op de hoogte te blijven van nieuwe dreigingen.
- Reset inloggegevens na patching: Roteer wachtwoorden en sleutels wanneer een kwetsbaarheid mogelijk tot blootstelling heeft geleid.
- Update firmware: Firmware-updates bevatten vaak belangrijke beveiligingsverbeteringen die niet in standaard patches zitten.

NEXT STEP 24 >

3. Harden infrastructure

Versterk de infrastructuur om de weerbaarheid te vergroten en een defense-in-depth strategie te ondersteunen.

- **Beperk beheerrechten: Blokkeer internet-toegankelijke beheerinterfaces en sta alleen toegang toe vanuit vertrouwde interne netwerken.**
- **Gebruik IP-gebaseerde filtering: Sta alleen toegang toe vanuit bekende en veilige regio's of IP-ranges.**
- **Filter botnetverkeer: Gebruik leveranciersregels om bekende kwaadaardige bronnen te blokkeren.**
- **Gebruik sterke encryptie: Pas veilige standaarden toe zoals AES-256 en schakel verouderde cipher suites uit.**

4. Versterk authenticatie-maatregelen

Aanvallen met gestolen of misbruikte inloggegevens blijven populair bij dreigingsactoren. Sterke authenticatie kan ongeautoriseerde toegang sterk verminderen.

- **Centraliseer authenticatie: Gebruik SSO en SAML via vertrouwde identity providers (IdP's).**
- **Controleer VPN-accounts: Verwijder regelmatig toegang voor inactieve gebruikers en externe partijen.**
- **Verplicht sterke multi-factor authenticatie: Gebruik phishing-bestendige methoden zoals hardware tokens met WebAuthn-standaarden.**
- **Stimuleer goede wachtwoordhygiëne: Gebruik sterke wachtwoorden, periodieke rotatie en wachtwoordmanagers.**

5. Monitor en log strategisch

Zichtbaarheid in edge-apparaten en gebruikersactiviteiten is cruciaal voor het detecteren en reageren op dreigingen.

- **Log zoveel mogelijk: Als je infrastructuur het toelaat zonder hoge kosten, log dan alles. Anders prioriteer logs die unieke zichtbaarheid bieden.**
- **Centraliseer logverzameling: Stuur logs naar externe systemen om manipulatie te voorkomen en onderzoek te ondersteunen.**
- **Gebruik gedragsanalyse: Detecteer laterale bewegingen en persistentiemechanismen die traditionele beveiliging omzeilen.**

NEXT STEP 24 >

6. Bevorder veilige softwarepraktijken

Gebruikersgedrag kan risico's introduceren, bijvoorbeeld door het downloaden van software uit onbetrouwbare bronnen.

- Informeer gebruikers: Maak hen bewust van risico's bij downloads via zoekmachines of onofficiële websites.
- Handhaaf softwarebeleid: Sta alleen software toe uit goedgekeurde interne of leverancierskanalen.

7. Monitor misbruik van vertrouwde platforms

Aanvallers gebruiken steeds vaker legitieme platforms om malware te verspreiden of activiteiten te verbergen.

- Let op misbruik van platforms: Monitor verkeer en gebruik van bijvoorbeeld GitHub, Google Ads en IT-toolrepositories.
- Ken je afhankelijkheden: Een supply chain-aanval kan jouw organisatie indirect raken via software-afhankelijkheden.

8. Beheer risico's van derde partijen

Externe leveranciers en dienstverleners hebben vaak toegang tot gevoelige systemen en data.

- Beoordeel de beveiliging van leveranciers: Neem security-eisen op in contracten en voer periodieke reviews uit.
- Beperk en monitor toegang: Pas het principe van least privilege toe en segmenteer externe verbindingen.

9. Implementeer netwerksegmentatie en Zero Trust

Platte netwerken maken het voor aanvallers gemakkelijker om lateraal te bewegen.

- Segmenteer kritieke systemen: Isoleer gevoelige omgevingen van algemene gebruikersnetwerken.
- Pas Zero Trust toe: Verifieer continu toegangsverzoeken en controleer vertrouwensniveaus.

NEXT STEP 24 >

10. Bereid incidentrespons en herstel voor

Goede voorbereiding verkleint de impact van incidenten en versnelt herstel.

- **Onderhoud en test IR-plannen: Zorg dat playbooks actueel zijn en regelmatig worden geoefend.**
- **Bescherm en test back-ups: Controleer of back-ups veilig, betrouwbaar en herstelbaar zijn.**
- **Definieer communicatieprotocollen: Betrek interne teams, juridische adviseurs en externe stakeholders.**

11. Maak optimaal gebruik van threat intelligence

Actuele en relevante threat intelligence helpt securityteams om dreigingen sneller te herkennen, beter te begrijpen en effectiever te reageren

- **Operationaliseer threat intelligence: Integreer intelligence-feeds in SIEM-, SOAR- en detectieprocessen.**
- **Gebruik contextuele verrijking: Pas threat intelligence toe om alerts beter te prioriteren en onderzoeken te ondersteunen.**
- **Werk samen met betrouwbare bronnen: Neem deel aan Information Sharing and Analysis Centers (ISAC's) of andere sectorgerichte samenwerkingsverbanden voor het delen van dreigingsinformatie.**

12. Bouw aan een security-bewuste organisatiecultuur

Technologie alleen is niet voldoende; mensen spelen een cruciale rol in beveiliging.

- **Voer regelmatig awareness-campagnes uit: Richt je op phishing, social engineering en veilig gedrag.**
- **Stem training af op rollen: Geef extra begeleiding aan risicogroepen zoals IT-admins en finance.**
- **Stimuleer melden van incidenten: Maak het eenvoudig en veilig voor medewerkers om verdachte activiteiten te rapporteren.**

NEXT STEP 24 >