ABN·AMRO

Detectie

Is uw IT-infrastructuur gehackt?

Cybercriminaliteit, een trend in opmars

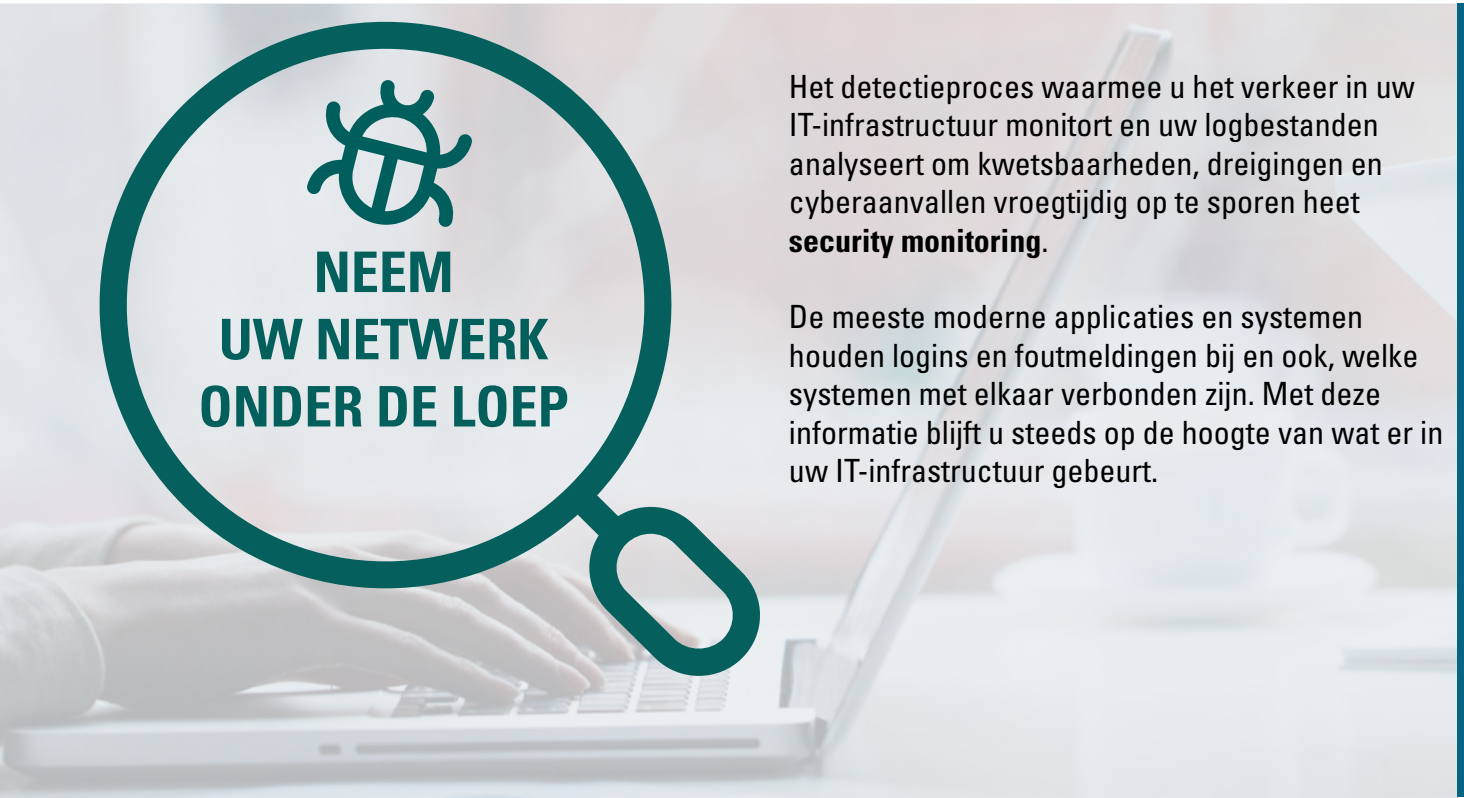
WEETJE

Bijna 2 van de 3
cyberaanvallen zijn gericht op het MKB[1].

1,2 miljoen $
bedraagt de gemiddelde schade aan de IT-infrastructuur door een cyberaanval of datalek[2].

ABN AMRO heeft in 2020 een toename gezien in het aantal en ook in de complexiteit van cyberaanvallen. Het maakt niet uit hoe groot uw bedrijf is, als uw bedrijfsvoering steunt op IT-systemen en applicaties bent u mogelijk interessant voor cybercriminelen, die steeds geavanceerder te werk gaan.

Wist u dat cybercriminelen zich maanden tot jaren onzichtbaar kunnen ophouden in uw netwerk? Met enkel preventieve securitymaatregelen bent u er dus niet. Om u te weren tegen digitale aanvallen, moet u zicht en grip hebben op de IT-infrastructuur en op wat er daarbinnen gebeurt. Dit artikel geeft u handvatten om de eerste stappen te zetten.



Het detectieproces waarmee u het verkeer in uw IT-infrastructuur monitort en uw logbestanden analyseert om kwetsbaarheden, dreigingen en cyberaanvallen vroegtijdig op te sporen heet **security monitoring**.

De meeste moderne applicaties en systemen houden logins en foutmeldingen bij en ook, welke systemen met elkaar verbonden zijn. Met deze informatie blijft u steeds op de hoogte van wat er in uw IT-infrastructuur gebeurt.

STELT U ZICH VOOR:

Op een dag haalt uw bedrijf het nieuws omdat uw klantdata op straat ligt. Blijkbaar hadden hackers toegang tot uw bedrijfssystemen.

Voordat een hacker uw data kan stelen, moet hij zich eerst door uw IT-infrastructuur bewegen. Plaatst u op de juiste plekken digitale alarmen, dan bent u al op de hoogte voor de media u benadert en kunt u passende maatregelen treffen. Mischien snijdt u de hacker zelfs wel de pas af.

Zonder inzicht in uw eigen IT-infrastructuur merkt u deze aanvallers vaak niet eens op.

1. computable.nl/boodschap-aan-mkb
2. keepersecurity.com/ponemon2019

Zet de eerste stappen

Het verzamelen en interpreteren van al deze technische data kan overweldigend zijn.

Heeft uw bedrijf een grote digitale voetafdruk? Dan is een SIEM-systeem misschien iets voor u. Daarmee kunt u op een centrale plek digitale alarmen instellen die u informeren zodra er verdachte handelingen plaatsvinden in uw IT-infrastructuur. Neem in uw overweging ook de investering mee in het personeel dat het SIEM zal beheren en de alarmen zal opvolgen. Als een SIEM-oplossing niet past kunt u gebruik maken van een decentrale oplossing. Vaak is er namelijk al een gebruiksklare alarmfunctie aanwezig in uw IT-beveiligingsproducten zoals uw antivirus, web security, mail security of uw firewall.

Hoe pakt u security monitoring praktisch aan?

1 Identificeer cruciale IT-systemen en applicaties

Dat kunnen uw e-commerce en bedrijfs-applicaties (zoals Microsoft 365), klant- en personeelsadministratie, routers en switches, firewalls en threat management-systemen (zoals uw antivirus-programma) zijn.

2 Definieer en installeer digitale alarmen

Digitale alarmen worden ook wel security monitoring use cases genoemd. Implementeer een basisset van algemene use cases voor uw cruciale IT-systemen en applicaties. Een voorbeeldlijst daarvan is in dit artikel te vinden. Voor specifieke use cases voor applicaties en systemen kan u uw IT-specialisten raadplegen.

3 Betrek uw IT-specialisten

Zij kunnen u helpen bij het definieren en installeren van de digitale alarmen en bij het interpreteren van inzichten uit de use cases. Zeker in het begin heeft uw bedrijf baat bij zowel de security- als de operationele verbeteringen die hieruit voortvloeien.

4 Breid uw verdedigingsarsenaal uit

Uw bedrijf groeit, en zo ook uw IT-landschap. Uw security monitoring moet dus dezelfde trend volgen. Naarmate u meer ervaren raakt, kunt u het aantal systemen, applicaties en het aantal use cases uitbreiden. Zo houdt u steeds een goed overzicht op de dreigingen voor uw IT-infrastructuur.

Welke dreigingen omzeilt u hiermee?

- × Ongeautoriseerde toegang tot uw bedrijfsdata
- × Misbruik van kwetsbaarheden in uw systemen
- × Lekken van vertrouwelijke data
- × Manipulatie van uw systemen
- × Ongeoorloofde handelingen in uw bedrijfsapplicaties
- × Niet-gemachtigde netwerkconnecties en onveilige netwerkprotocollen

Wat zijn de voordelen?

- \+ Direct inzicht in uw IT-Infrastructuur
- \+ Ondersteuning bij het bepalen van risico's
- \+ Versneld oplossen van veiligheidsrisico's
- \+ Vertrouwen van uw klanten
- \+ Proactieve in plaats van reactieve houding
- \+ Naleving van relevante wet- en regelgeving
- \+ Betere verzekeringstarieven
- \+ Hulp bij het prioritizeren van maatregelen

Gebruik deze scenario's als startpunt

Misbruik van hoge toegangsrechten van gebruikers

- Foutieve inlogpogingen van beheeraccounts
- Nieuwe of ongebruikelijke inlogpogingen van beheeraccounts

Valideer gebruikers en inlogpogingen en ontneem toegangsrechten en/of wijzig wachtwoord indien nodig.

Vertrouwde systemen

- Nieuwe systemen die in uw netwerk gevonden worden of zijn toegevoegd
- Systemen die verdwijnen van uw netwerk

Verifieer en autoriseer systemen en zorg dat ze opgenomen worden in het asset overzicht . Verwijder ongeautoriseerde systemen.

Verbergen van aanvalssporen

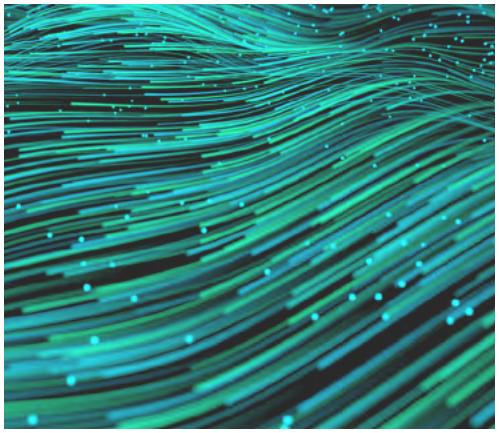
- Het uitzetten van logboekregistratie op systemen of applicaties
- Het verwijderen of aanpassen van logbestanden
- Het aanpassen van loginstellingen

Wat is de reden voor het uitzetten of wijzigen van de loginstellingen? Is dit een legitieme wijziging? Kan de gebruiker dit verantwoorden? Herzie de loginstellingen.

Detectie van verdachte bestanden

- Antivirus detecteert malware op één van uw systemen
- Antivirus is niet in staat om de malware te verwijderen

Ontkoppel het systeem van het netwerk indien mogelijk en verwijder de malware van het systeem. U kunt een herinstallatie overwegen om er zeker van te zijn dat de malware van het systeem af is.



Ongeautoriseerde toegang tot publieke systemen

- Toegang tot ongebruikelijke websites
- Cloudopslag publiekelijk toegankelijk (bijvoorbeeld S3, Google Drive, Dropbox)

Pas toegangsrestricties toe voor ongeautoriseerde websites of groepen (bijvoorbeeld drugs, gokken) en herzie access control en permissies van uw cloudopslag.

Het gebruik van onveilige of niet toegestane services

Het gebruik van afwijkende services (bijvoorbeeld ftp, ssh, telnet) om externe systemen te benaderen vanuit uw intern netwerk

Creëer een overzicht van de services die nodig zijn voor uw bedrijfsvoering en inventariseer de uitzonderingen. Blokkeer ongewenste combinaties in overleg met uw IT-afdeling.

Ongeautoriseerde toegang tot interne systemen

Ongebruikelijke toegangspogingen tot interne systemen

Valideer toegangspogingen. Verleen alleen de toegang aan de gebruikers die dit nodig hebben voor werkzaamheden.

De bovenstaande lijst is geen uitputtende lijst. Hij is bedoeld als startpunt voor uw bedrijf.

WEETJE

ABN AMRO vindt het belangrijk dat u veilig kan zakendoen, en dat u gratis tools ter beschikking hebt die u daarbij kunnen helpen. Daarom hebben we meegeholpen aan de ontwikkeling van het Magma UC Framework[3], een framework voor de continue ontwikkeling van use cases.

3. betaalvereniging.nl/veiligheid

Groei door naar succes

1.
Verdachte gebeurtenissen opsporen

Met deze pragmatische security monitoring-aanpak kunt u de eerste stappen zetten in het detecteren van verdachte gebeurtenissen.

2.
Verbeteringen voorstellen

Er doen zich ongetwijfeld gebeurtenissen voor die u kan gebruiken om verbeteringen voor te stellen en zo de volwassenheid van uw cyberbeveiliging naar een hoger niveau te tillen.

3.
Oplossingen aanbieden

Heeft u verbeteringen geidentificeerd, dan moeten ze worden opgevolgd. Ook moeten er misschien auditresultaten opgelost worden.

4.
Wet- en regelgeving nakomen

Het resultaat van deze inspanningen loont de moeite: U zal waarschijnlijk al voor een groot deel voldoen aan de voor u relevante wet- en regelgeving, zoals GDPR, PCI-DSS, HIPAA en SOX.

Wat kunt u nog meer doen?

Aanvallers detecteren is één van de onderdelen van de strijd tegen cyberdreigingen. Andere onderdelen zijn:

- Weet wat u moet beschermen
- Weet wat er op u af komt

Vind op onze website[3] meer informatie over hoe de bank u kan helpen de risico's te beheersen.

Vergeet ook niet 'De 9 cybersecurity essentials voor MKB in 2020'[4] te lezen, vol met praktische tips voor het beveiligen van uw bedrijf en het beschermen van uw werknemers.

4. abnamro.nl/cyber
5. 9 cybersecurity essentials

Woordenlijst

Cyberaanval	Een opzettelijke poging, vaak met kwade bedoelingen, door één of meerdere personen om in uw IT-systemen in te breken
Cybercriminaliteit	Een verzamelnaam voor alle vorm van criminaliteit met IT als middel en doelwit
Cybercrimineel	Individu of groep die computercriminaliteit bedrijft; computercrimineel; internetcrimineel
Datalek	Het opzettelijk of onopzettelijk naar buiten komen van vertrouwelijke gegevens, zodat derden toegang hebben tot uw gegevens
Digitale voetafdruk	Herleidbare digitale activiteiten of handelingen die middels het internet of digitale apparaten (zie ook IT-infrastructuur) worden uitgevoerd
IT-infrastructuur	Al uw hardware, software, netwerken en andere faciliteiten die gebruikt worden om u applicaties en IT-diensten te leveren
Kwetsbaarheid	Zwakke plekken in uw IT-infrastructuur waar cybercriminelen gebruik van maken om hun doelstelling te bereiken
Netwerkconnectie	De digitale communicatie die tussen IT-systemen plaatsvindt en nodig is voor de correcte werking van uw systemen/applicaties. De connecties maken gebruik van diverse protocollen, met ieder een ander doel.
Onveilige netwerkrotocol	Een afgesproken voorschrift van communicatie binnen een netwerk, maar één waarbij belangrijke functies ontbreken, zoals bijvoorbeeld de versleuteling op de netwerkconnectie waardoor het voor cybercriminelen mogelijk is om uw wachtwoorden relatief eenvoudig af te vangen
Security monitoring	Het gehele detectieproces van verdachte situaties in uw IT-infrastructuur, vanaf het definiëren van digitale alarmen tot aan het analyseren van alarmen en het nemen van passende stappen
SIEM	Afkorting voor “security information and event management”, een veiligheidsmaatregel die wordt ingezet voor het centraal verzamelen en verwerken van logbestanden. Dankzij digitale alarmen krijgt u real-time inzicht in verdachte situaties binnen uw IT-infrastructuur.
Use case	Methode om digitale bedrijfsbedreigingen te koppelen aan meerdere digitale alarmen in uw SIEM-oplossing; vaak een functionele omschrijving van wat u tracht te detecteren zoals ongeautoriseerde toegang tot uw IT-systemen of ransomware