Hoe herken ik een cyberaanval op mijn bedrijf?

https://aucuba.nl/kennisbank/uncategorized/hoe-herken-ik-een-cyberaanval-op-mijn-bedrijf/

Een cyberaanval herken je aan onverwachte systeemvertragingen, vreemde inlogpogingen, onbekende bestanden of software, en plotselinge toegangsproblemen tot je eigen gegevens. Deze signalen zijn niet altijd meteen zichtbaar, wat aanvallen gevaarlijk maakt. In dit artikel beantwoorden we de meest gestelde vragen over het herkennen van cybercrime, zodat jij als ondernemer weet waar je op moet letten.

Wat zijn de eerste tekenen van een cyberaanval?

De eerste tekenen van een cyberaanval zijn vaak subtiel: systemen die trager werken dan normaal, programma's die onverwacht crashen, onbekende software die ineens actief is, of medewerkers die melden dat ze niet meer bij hun bestanden kunnen. Deze signalen lijken soms op gewone technische problemen, maar een combinatie van meerdere symptomen tegelijk is een serieuze waarschuwing.

Andere vroege signalen die je alert moeten maken zijn onder andere:

- Onverwachte wachtwoordwijzigingen of vergrendelde accounts
- Onbekende inlogpogingen, zeker buiten werktijden
- Bestanden die zijn hernoemd of niet meer te openen zijn
- Ongewone e-mails die vanuit jouw bedrijfsaccount worden verzonden
- Plotseling hoog dataverbruik zonder duidelijke oorzaak

Het gevaar is dat veel aanvallen bewust onder de radar blijven. Cybercriminelen willen zo lang mogelijk onopgemerkt blijven om zoveel mogelijk informatie te verzamelen of schade aan te richten. Hoe eerder je een beveiligingsincident herkent, hoe beperkter de schade blijft.

Hoe weet je of je bedrijfsgegevens zijn gestolen?

Je bedrijfsgegevens zijn mogelijk gestolen als je onverwachte toegangspogingen ziet in logbestanden, als klanten melden dat ze verdachte berichten ontvangen die van jou afkomstig

lijken, of als vertrouwelijke informatie opduikt op plekken waar die niet thuishoort. Datalekken zijn helaas vaak pas achteraf zichtbaar.

Een aantal concrete aanwijzingen dat gegevens zijn buitgemaakt:

- Klanten of leveranciers ontvangen phishingmails die jouw bedrijfsnaam gebruiken
- Inloggegevens van medewerkers circuleren op het dark web
- Interne documenten of klantgegevens zijn op onbekende locaties opgeslagen
- Financiële transacties die niemand herkent

Wil je actief controleren of jouw zakelijke e-mailadressen zijn gelekt, dan bestaan er tools die dit voor je checken aan de hand van bekende datalekken. Preventieve monitoring is echter betrouwbaarder dan achteraf zoeken. Proactief beheer van je netwerk maakt het mogelijk om verdacht dataverkeer vroegtijdig te detecteren.

Wat is het verschil tussen een virus, ransomware en phishing?

Een virus is kwaadaardige software die zichzelf verspreidt en schade aanricht aan bestanden of systemen. Ransomware is een specifieke vorm van malware die je bestanden versleutelt en losgeld eist voor de toegang. Phishing is geen software, maar een misleidingstechniek waarbij criminelen zich voordoen als een betrouwbare partij om inloggegevens of geld te ontfutselen.

Virus en malware

Een virus nestelt zich in bestanden of programma's en verspreidt zich verder zodra die worden geopend of gedeeld. Het doel kan variëren van het beschadigen van systemen tot het stelen van gegevens. Malware is de overkoepelende term voor alle vormen van kwaadaardige software, waaronder virussen, spyware en ransomware.

Ransomware en phishing

Ransomware vergrendelt je bestanden of systemen volledig. Je krijgt een melding dat je moet betalen om weer toegang te krijgen, maar betalen biedt geen garantie op herstel. Phishing gebeurt via e-mail, sms of nepsites en is gericht op het misleiden van mensen, niet op het infecteren van systemen. Toch is phishing vaak de ingang voor een grotere aanval: een medewerker klikt op een link en opent zo de deur voor malware of ransomware.

Waarom zijn MKB-bedrijven een aantrekkelijk doelwit voor cybercriminelen?

MKB-bedrijven zijn aantrekkelijk voor cybercriminelen omdat ze waardevolle bedrijfsgegevens bezitten, maar doorgaans minder beveiligd zijn dan grote ondernemingen. Ze hebben zelden een eigen IT-afdeling, minder geavanceerde beveiligingstools en minder bewustzijn bij medewerkers over cyberdreigingen. Dat maakt ze een relatief eenvoudig doelwit met een hoge slagingskans.

Cybercriminelen zijn pragmatisch: ze kiezen de weg van de minste weerstand. Een groot bedrijf met een volledig beveiligingsteam is moeilijker te kraken dan een MKB-bedrijf met verouderde software en geen monitoringssysteem. Bovendien verwerken veel MKB-bedrijven gevoelige klant- en financiële gegevens, wat hen waardevol maakt als doelwit.

In 2026 zien we dat aanvallen op het MKB steeds gerichter worden. Criminelen doen vooraf onderzoek naar bedrijven, hun medewerkers en hun systemen. Een gepersonaliseerde phishingmail gericht aan de directeur of financieel medewerker is veel effectiever dan een generieke aanval. Cyberbeveiliging voor het MKB is daarmee geen luxe meer, maar een noodzaak.

Wat moet je doen als je een cyberaanval vermoedt?

Als je een cyberaanval vermoedt, moet je direct handelen: koppel het getroffen apparaat los van het netwerk, wijzig wachtwoorden van kritieke accounts, informeer je ICT-verantwoordelijke of externe partner, en documenteer wat je hebt gezien. Snel ingrijpen beperkt de verspreiding en de schade aanzienlijk.

Volg bij een vermoeden van een beveiligingsincident deze stappen:

1. **Isoleer het getroffen systeem** door het los te koppelen van het netwerk en internet.
2. **Verander wachtwoorden** van e-mail, bedrijfssoftware en andere kritieke accounts, bij voorkeur vanaf een niet-getroffen apparaat.
3. **Neem contact op met je ICT-partner** zodat er direct onderzoek kan worden gedaan.
4. **Documenteer de situatie**: wat heb je gezien, wanneer, op welk apparaat?
5. **Meld het incident** indien nodig bij de Autoriteit Persoonsgegevens, zeker als er klantgegevens bij betrokken zijn.

Wat je niet moet doen: proberen het zelf op te lossen zonder expertise, of het incident intern houden uit angst voor reputatieschade. Hoe sneller professionele hulp wordt ingeschakeld, hoe

groter de kans op volledig herstel.

Hoe voorkom je dat een cyberaanval onopgemerkt blijft?

Je voorkomt dat een cyberaanval onopgemerkt blijft door actieve monitoring van je netwerk, regelmatige controle van inlogactiviteiten en het trainen van medewerkers om verdachte situaties te herkennen en te melden. Proactieve bewaking is de enige betrouwbare manier om aanvallen vroeg te detecteren.

Concrete maatregelen die het verschil maken:

- **Netwerkmonitoring:** automatische bewaking signaleert afwijkend dataverkeer direct.
- **Logbeheer:** inlogpogingen en systeemactiviteiten worden bijgehouden en geanalyseerd.
- **Medewerkerstraining:** bewustzijn over phishing en social engineering vermindert het risico op menselijke fouten.
- **Regelmatige updates:** verouderde software bevat kwetsbaarheden die actief worden misbruikt.
- **Tweefactorauthenticatie:** een extra verificatiestap maakt het stelen van inloggegevens minder effectief.

Wij helpen MKB-bedrijven met proactief beheer en continue monitoring, zodat afwijkingen direct worden gesignaleerd en opgepakt voordat ze uitgroeien tot een serieus incident. Wil je weten hoe jouw bedrijf er nu voor staat op het gebied van cyberbeveiliging? Neem gerust contact met ons op voor een vrijblijvend gesprek.