mevas

STERK VERZEKERINGSWERK

Perfect Day

Perfect Day

SINDS 2019

Wij helpen MKB bedrijven de basisveiligheid op orde te krijgen die nodig is om de bedrijfscontinuïteit te waarborgen in de digitale wereld.

Programma

- Aannames cybercrime
- Waarom elk bedrijf risico's loopt
- Jezelf wapenen
- Basisveiligheid op orde brengen

Cybercrime

“Cybercrime zijn misdaden die gepleegd worden met een ICT-middel, dus een computer, smartphone, smartwatch of tablet, gericht op een ander ICT-middel.”

Cyber incidenten

“Cyber incidenten zijn veiligheidsincidenten waarbij informatie, systemen, netwerken, of diensten worden aangetast door ongeautoriseerde acties, **vaak** met kwade intenties.”

Cyberrisico’s

Het gaat om de gevolgen

Cyberincidenten

- Verwijderen van gegevens
- Shadow-IT
- Verloren apparaten
- Delen van gegevens

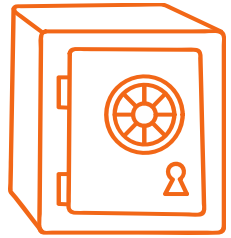
Cybercrime

- Versleutelen van gegevens
- Stelen van data
- Verkrijgen inloggegevens
- Spionage

Hardnekkige aannames Cybersecurity

Mijn IT’er regelt dit!

Alles staat in de Cloud!



Ik ben niet interessant, bij mij valt niets te halen!

Waarom élk bedrijf risico loopt

‘Ik ben niet interessant voor hackers’ ‘Ik heb geen gevoelige data’

De vraag is niet:

“Wat valt er bij mij nou te halen?”

De vraag is:

“Wat kost het mij als ik niet verder kan?”

Jezelf wapenen

Zorg voor de basishygiëne

Inventariseren

- Netwerk in kaart
- Processen in kaart
- Waar zitten de risico's
- Keten in kaart brengen
- Welke stappen moet je nog zetten

Basismaatregelen

- Technische maatregelen
- Fysieke toegang
- Organisatorische maatregelen en beleid
- Noodprocedure
- Faciliteren van afspraken en beleid

Trainen

- Onboarding en offboarding
- Bewustzijn medewerkers
- Nood / incidentenplan oefenen

Evalueren

- Werkt de noodprocedure
- Zijn alle documenten nog up-to-date
- Zijn er veranderingen en nieuwe dreigingen
- Is er een risico waarbij een verzekering kan helpen

Hoe ze bij je binnenkomen

En hoe je al veel kunt voorkomen met **technische** maatregelen

Aanval	Verdediging
• Nestelen in netwerk • Beveiligingslekken • Misbruik van wachtwoorden • Malware en virus • Legacy apparaten en applicaties	• Netwerk beveiligen (firewall, SOC) • Updaten & patchmanagement • Wachtwoordbeleid en MFA • Virusbescherming • Inventariseren IT-landschap en opslag

Hoe ze bij je binnenkomen

En hoe je al veel kunt voorkomen met **organisatorische** maatregelen

Aanval	Verdediging
• Social engineering • Via de keten • Toegang tot alle gegevens • Misbruik van wachtwoorden • Via privé-apparaten	• Trainen van personeel • Inventariseren en ketenafspraken • Beheer van toegangsrechten • Wachtwoordbeleid en MFA • BYOD-beleid

De cyber security audit

De 0-meting

Medewerkers

Techniek (IT & OT)

Wetgeving AVG

Noodprocessen

Ketenveiligheid

Scan e-mail & website

Het rapport

CYBERADVIES

SCORE

Je ziet hier de overall score van het bedrijf per thema. De uitwerkingen en aanbevelingen per thema vind je op de volgende pagina's.

MEDEWERKERS

Je kunt nog veel verbeteren aan het bewustzijn en veiligheid van medewerkers, met name in de productiehal. Denk daarbij aan algemene awareness, wachtwoordbeleid en 2FA.

KRITIEK

TECHNIEK

De techniek op het kantoor (IT) is grotendeels op orde, echter in de productiehal (OT) niet. Daar zijn belangrijke verbeteringen nodig, met name segmentatie van het netwerk, back-ups en veilige (API)koppelingen.

ONVEILIG

WETGEVING

De AVG is deels op orde. Kijk nog naar de benodigde registers en sluit met alle partijen een verwerkersovereenkomst af. Zet jullie privacyverklaring op de website.

ONVOLDOENDE

NOODPROCES

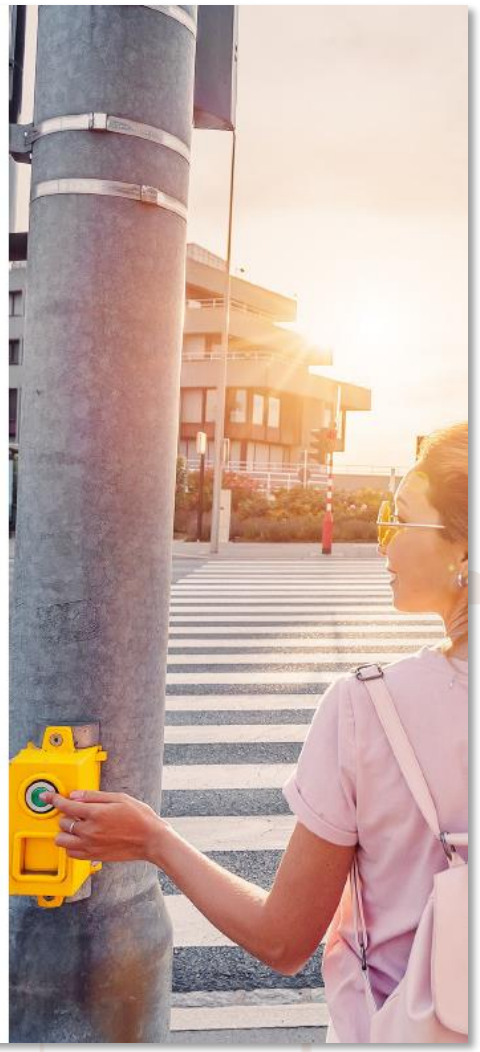
De medewerkers weten welke leveranciers ze moeten bereiken bij een cyber incident, ook als het gaat om de operationele techniek (OT). Er is een bellijst met noodnummers en een plan voor een datalek.

GOED

KETENVEILIGHEID

Er is inzicht in de ketenveiligheid. Met de leveranciers en afnemers zijn (onderhouds)contracten afgesloten. De impact op het productieproces bij een cyber incident is niet bekend. Voer een risicoanalyse uit.

KAN BETER



Het rapport

TECHNIEK

Installeer een certificaat op de website en beveilig de beheerpagina.

ONVEILIG: Je websitebezoekers lopen het risico gehackt te worden als je niet de meest actuele internetstandaarden toepast. Als zij bijvoorbeeld via een contactformulier op je website gegevens naar jou verzenden, kunnen criminelen deze gegevens onderscheppen als deze niet (goed) versleuteld zijn.

Wij hebben de website van buitenaf gecheckt op een aantal standaard beveiligingsmaatregelen. Goed dat jullie een certificaat geïnstalleerd hebben, maar we zien hier nog veel verbeteringen mogelijk. De volgende zaken staan niet (goed) ingesteld: DNSSEC, de automatische verwijzing naar de beveiligde (HTTPS) versie, HSTS, het gebruik van een verouderde TLS versie (versie 1.0 of 1.1) en de betrouwbaarheid of de geldigheidsduur van de certificaat (chain), Wij raden aan deze opties te gaan ondersteunen of te verbeteren. Vaak is dit vrij eenvoudig te regelen door de websitebouwer, de hostingspartij en/of de partij die jullie domein(en) beheert. De beheerpagina blijkt ook niet extra beschermd te zijn. De beheerpagina is via het internet toegankelijk. We adviseren hier minimaal een Captcha beveiliging op te zetten om geautomatiseerd inloggen tegen te gaan, maar het liefst zien we hier ook 2FA en/of whitelisting.

WETGEVING

Ga aan de slag met de AVG en leg de benodigde registers aan.

ONVEILIG: Voldoe je niet aan de AVG dan riskeer je hiermee een boete van de Autoriteit Persoonsgegevens (AP). Deze boete kan oplopen tot 4% van je jaaromzet. De AP kan al een onderzoek instellen naar aanleiding van een klacht van slechts 1 klant.

Goed dat jullie i.v.m. de AVG een privacyverklaring aangelegd hebben. Wij hebben deze gecontroleerd en deze voldoet aan de gestelde eisen. Wij raden aan om verder met de AVG aan de slag te gaan. De AVG stelt ook eisen aan hoe jullie om moeten gaan met persoons- en klantgegevens. Inventariseer waar jullie deze gegevens allemaal opslaan en met welke reden en leg dit vast in een verwerkersregister. Jullie dienen een datalekregister aan te leggen waarin jullie bijhouden wat er met betrekking tot de gegevens fout is gegaan.

Na het rapport

Perfect Day dienstverlening

Organisatie

- Aanpak verbeterpunten
- Phishingmails
- Trainingen & opleiding
- Periodiek contact

Techniek

- Vulnerabilityscan netwerk
- Websitescan
- Pentests
- Contact met IT

Documentatie

- AVG Documentatie & ondersteuning
- Beleidsdocumenten
- Begeleiding Noodplan

Security audit

0-meting met rapport

50% vergoed door MEVAS in 2025*

Small	Medium	Large
t/m 9 medewerkers	10-29 medewerkers	30+ medewerkers
~~€795,-~~ €675,-**	~~€995,-~~ €850,-**	~~€1295.-~~ €1100,-**

* De factuur wordt naar je bedrijf gestuurd, je betaalt deze dus zelf. Als je de factuur vervolgens naar Mevas stuurt storten zij de helft van het factuurbedrag weer op je rekening.

** Deze speciale prijs met korting van 15% geldt voor Mevas-leden

Perfect Day

Plan nu een afspraak
voor de cyber scan

Heb je nog een beetje overtuiging nodig?

Je kunt ook eerst een gratis 15 minuten intake met een cyber expert aanvragen.

E: contact@perfectday.nl

T: 085 048 61 09

www.perfectday.nl