Perfect Day

Eenvoudig en betaalbaar beschermd tegen cybercriminaliteit

Inhoudsopgave

Al langere tijd neemt cybercriminaliteit onder mkb-bedrijven toe. Niet langer zijn alleen multinationals doelwit, maar gaan criminelen voor het laaghangende fruit: matig beveiligde kleine- en middelgrote ondernemingen. Perfect Day helpt jou je bedrijf te beschermen. Met betaalbare, praktische oplossingen. Speciaal ontworpen voor het mkb.

Wat valt er nou bij mij te halen?

Dit horen wij heel vaak, maar juist om die reden zo gevaarlijk: wat een cybercrimineel bij jou steelt, lekt of gijzelt is voor hem waarschijnlijk niet belangrijk, maar voor jou en jouw bedrijf vaak cruciaal. En dát weet die anonieme hacker aan de andere kant van de wereld. Want dat is precies wat het internet ook mogelijk maakt: een cybercrimineel controleert van duizenden kilometers afstand moeiteloos of jij je beveiliging op orde hebt. Hackers scannen continu het hele internet af op zoek naar de zwakke plekken. Vinden ze bij jou een zwakke plek? Dan gaan ze vervolgens gericht te werk en proberen ze bij je binnen te komen. En als ze eenmaal binnen zijn, dan kijken ze pas wie of welk bedrijf erachter zit.

Het is tijd om met een bredere blik naar digitale veiligheid te kijken en te erkennen dat cyber- en data security een gedeelde verantwoordelijkheid van iedereen binnen het bedrijf is en niet alleen van de IT. **En het goede nieuws? Dat is lang niet zo moeilijk als het klinkt.** Met relatief eenvoudige aanpassingen en een andere mindset, kom je al een heel eind.

Perfect Day

Cyber Security
volgens onze experts

Wij benaderen cyber security als het geheel van alle aspecten die invloed kunnen hebben op de digitale veiligheid van jouw bedrijf, jouw systemen, data en productieproces. Daarom baseren wij onze dienstverlening op vijf pijlers:

Medewerkers

Techniek (IT & OT)

Wetgeving AVG

Noodprocessen

Ketenveiligheid

OT staat voor operational technology, oftewel de systemen die worden gebruikt om operationele processen in de fysieke wereld aan te sturen. Denk bijvoorbeeld aan machines in een fabriek, de sprinklers in een kas, maar ook aan kassasystemen, camera's en IoT (Internet of Things).

Bij cyber security denken veel mensen alleen aan techniek. Maar wist je dat 95% van alle hacks en datalekken aan een menselijke fout zijn toe te wijzen? Belangrijk dus om te investeren in veilige processen in combinatie met kennis en bewustzijn bij medewerkers.

Wij helpen jou bij het beschermen van je bedrijf

Cyber security is geen leuk onderwerp binnen het ondernemen en het kost tijd en geld, maar het moet wel gebeuren. Cyberincidenten vormen bedreiging nummer 1 voor de bedrijfscontinuïteit van mkb-bedrijven. Neem eens een moment de tijd om te bedenken welke consequenties het heeft als al jouw systemen en apparaten niet meer bereikbaar zijn. Of als je klant- of personeelgegevens op straat liggen? Dat kost veel meer tijd en geld dan het vooraf op orde brengen van je cyber security.

Perfect Day helpt jou je bedrijf beter te beschermen tegen:

- Hacks, malware, DDoS aanvallen en ransomware;
- Phishing, CEO Fraude en social engineering;
- Datalekken, spionage, verlies van data en gestolen data;
- Inbraak in systemen of (productie) apparaten en machines, cryptomining.

Veel mkb-bedrijven hebben pottenkijkers in de systemen, vaak is dat ongemerkt. Criminelen nemen rustig de tijd om te bekijken wat er allemaal in jouw systemen omgaat, wat voor data je in je bezit hebt en hoe de betaalprocessen lopen. Ze kunnen op ieder moment besluiten om hun buit te komen verzilveren. Bijvoorbeeld door al je bestanden te versleutelen en in ruil voor losgeld pas weer te ontsleutelen. Of door gevoelige informatie te verkopen op het Darkweb. Het duurt gemiddeld 198 dagen voordat je doorhebt dat je gehackt bent.

Onze oplossingen
de basis in drie stappen op orde

Voorkomen is beter dan genezen. Zeker als het gaat om digitale veiligheid. Daarom bestaat onze hulp uit een combinatie van inzicht, advies en oplossingen.

Security Pakket

- Externe vulnerability scan van netwerk, e-mail & website
- Phishing tests onder de medewerkers
- AVG documentatie
- Noodlijn voor incidenten
- Richtlijnen voor noodplan & preventiekaarten
- Beleidsdocumenten
- Signaleren van nieuwe bedreigingen & proactief informeren
- Periodiek overleg met cyber expert als vast aanspreekpunt

Hoe werkt het?

Stap 1 De 0-meting: cyber security audit & rapport. We brengen alle onderdelen van de cyber security in kaart en leveren een rapport met de risico's en verbeterpunten aan.

Stap 2 De basis op orde: we pakken de verbeterpunten uit het rapport aan, scannen je netwerk en website van buitenaf, gaan aan de slag met medewerker awareness door middel van phishing tests én we brengen de AVG en noodproces op orde.

Stap 3 Actieve samenwerking: we pakken de security aan en hierbij heb je periodiek contact met je cyberexpert. Je krijgt een cyber expert als vast aanspreekpunt voor advies en ondersteuning. We bespreken de voortgang, de security prioriteiten, de resultaten van de vulnerability scans en phishing tests en we houden je op de hoogte van potentiële dreigingen en vereiste updates.

Basis op orde bespaart tijd, geld en zorgen. Gun jezelf een Perfect Day!

Prijzen
van onze oplossingen

Hoe veilig is jouw bedrijf? We starten met een cyber security audit om dat te bepalen. De actiepunten uit de audit pak je direct aan met het security pakket. Daarin zit een effectieve mix van expert hulp en de juiste producten die we precies op jouw behoeften kunnen afstemmen.

Security audit

Small	Medium	Large
t/m 9 medewerkers	10-29 medewerkers	30+ medewerkers
€ 795,-	**€ 995,-**	**€ 1295,-**

Security pakket

Small	Medium	Large
tot 9 medewerkers	10-29 medewerkers	30+ medewerkers
€ 1195,- p.j.	**€ 1595,-** p.j.	**€ 1995,-** p.j.

** Alle prijzen zijn excl. BTW*

Wat onze klanten zeggen:

Perfect Day: een goede ervaring!

Perfect Day heeft een cyber security audit bij ons uitgevoerd. Dat was een goede ervaring: een prettige gesprekspartner met kennis van zaken en een duidelijk en overzichtelijk rapport met de risico's en concrete aanbevelingen waarmee we direct aan de slag konden gaan. Met de geboden oplossingen konden we meteen grote stappen zetten in de beveiliging.

Echt blij dat ik dit gedaan heb

Echt blij dat ik dit gedaan heb. Je hoort en leest zo veel dingen mis kunnen gaan, maar ik had geen idee waar te beginnen. Je wordt stap voor stap door de belangrijkste zaken heen geleid en geholpen met een oplossing. Ik zie het als een professionaliseringsslag voor mijn bedrijf dat ik dit heb gedaan.

Perfecte audit!

Via een prettig gesprek gaan ogen open. Waar je denkt het redelijk op orde te hebben, komen er toch wat aandachtspunten boven water. En daar was het om te doen. De bevindingen van het gesprek zijn in een helder rapport weergegeven. Makkelijk om de vervolg-stappen te ondernemen. Dus zeer waardevol.

*Wij krijgen van onze klanten de rating **uitstekend** op Trustpilot.*

Praktijkvoorbeelden van cybercriminaliteit

Groothandel

Een grote vleesleverancier regelt de temperatuur van zijn koelcellen op afstand. Hackers weten zijn netwerk binnen te dringen en voeren de temperatuur een graad of 30 op. De slager kan al zijn vlees weggooien, hij kan niet leveren aan zijn klanten en als kers op de taart krijgt hij alleen weer toegang tot zijn eigen systemen als hij de criminelen betaalt.

Zorg

Een medewerker van een keten van tandartsenpraktijken opent een link in een e-mail van een leverancier. Hiermee geeft zij een hacker toegang tot het computersysteem en patiëntgegevens. Naast gevoelige medische gegevens, bevatten de bestanden informatie als namen, adressen, polisnummer van de verzekering en betalingen. De hacker verkoopt de gegevens op de zwarte markt en ze worden onder meer gebruikt voor identiteitsfraude.

Bouw

Een aannemer werd meer dan een ton afhandig gemaakt door een datalek bij zijn accountant. Criminelen wisten uit dat lek de inloggegevens van zijn online boekhoudpakket te achterhalen en veranderden de gegevens van zijn leveranciers zo dat alle facturen aan hen uitbetaald werden. Dit kwam aan het licht nadat leveranciers hem als wanbetaler begonnen te behandelen.

Webshop

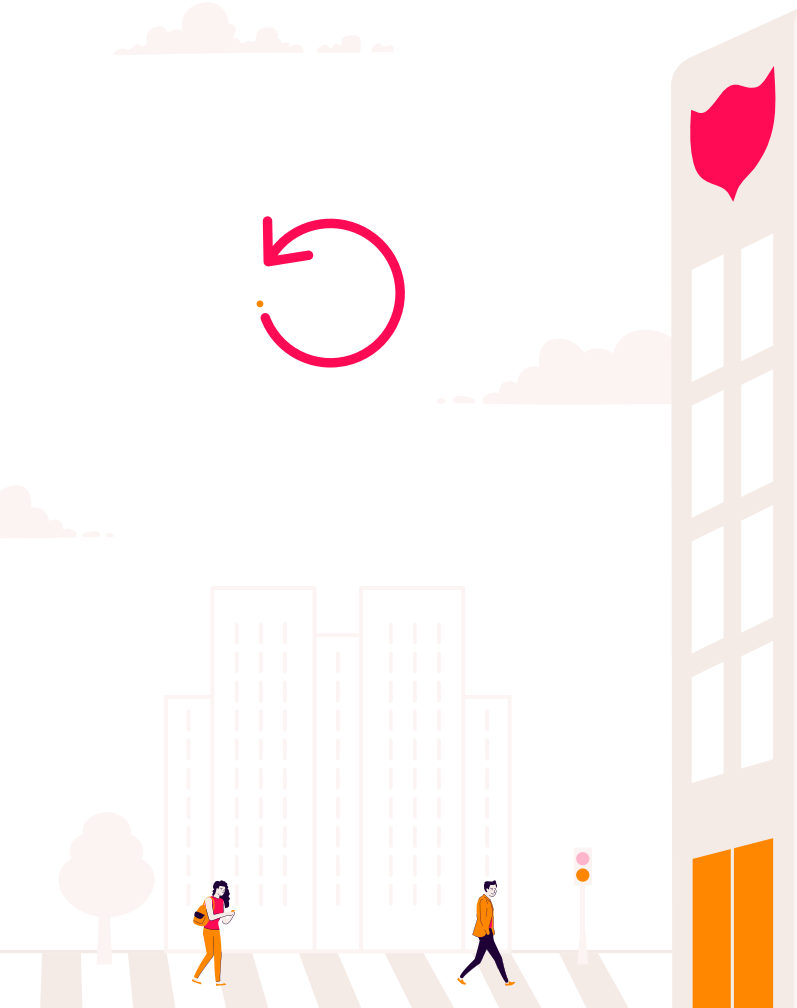
Door een hack bij een populaire webshop liggen de wachtwoorden en privégegevens van bijna 4 miljoen Nederlanders op straat. De gegevens zijn verkocht via een hackersforum en er wordt nu actief misbruik van gemaakt. De webshop wordt verweten dat ze aantoonbaar een zwakke beveiliging hadden en niet zorgvuldig met de privégegevens van alle klanten en prospects zijn omgegaan. Naast de enorme reputatieschade die het bedrijf oploopt, is de kans groot dat dit een vervelend juridisch staartje krijgt.

Rechtskundig

Door een hack bij een grote IT-leverancier kan een derde van alle Nederlandse notariskantoren in een klap niet meer werken. Ze sluiten uit voorzorg hun servers en databases omdat de hackers via de leverancier mogelijk toegang krijgen tot hun eigen systemen. Een aantal grote notariële software leveranciers heeft hetzelfde gedaan. Zo ligt een hele keten door de hack bij één partij plat. De notariskantoren hebben geen toegang tot contactgegevens en kunnen hun klanten dus niet informeren over de gevolgen voor hun afspraken en akten.

Transport

Hackers gijzelden het computernetwerk van een logistiek dienstverlener. Nadat de criminelen ervoor zorgden dat systemen niet meer functioneerden en bestanden versleuteld waren, konden de medewerkers op kantoor niet meer werken. Chauffeurs wisten hun route niet en keerden met volle wagens terug naar de thuisbasis. De schade liep in de papieren, boze klanten vroegen zich af waar hun leveringen bleven. Uiteindelijk besloot het bedrijf toch maar losgeld te betalen om zo snel mogelijk weer verder te kunnen.



Perfect Day

Plan nu een afspraak
voor de cyber security audit

Heb je nog meer overtuiging nodig?

Vraag dan eerst een gratis 15 minuten intake aan

E: contact@perfectday.nl

T: 085 048 61 09

www.perfectday.nl

Perfect Day is een initiatief van Nationale-Nederlanden.