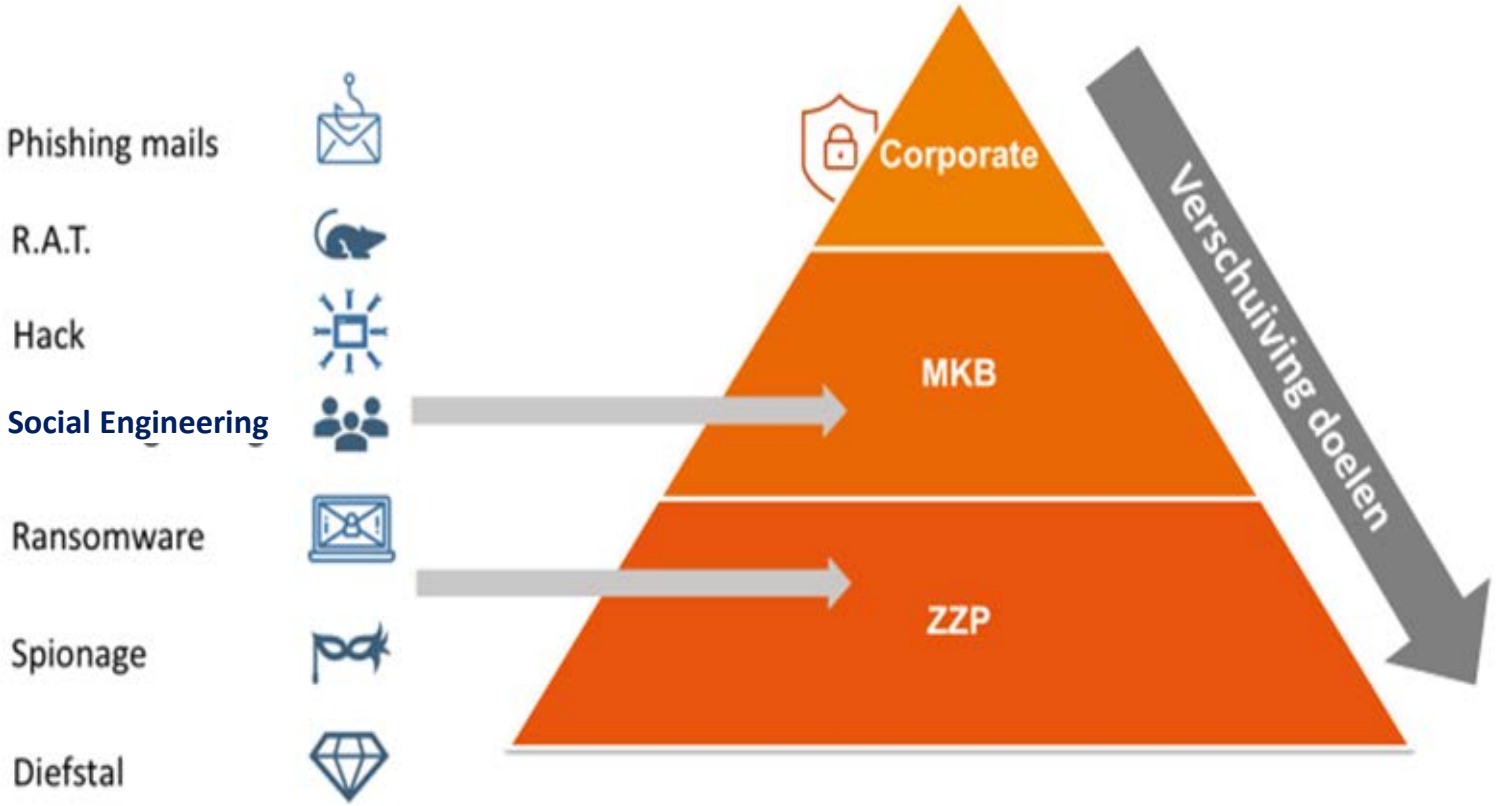
What the hack?!
Hoe digitaal veilig is jouw bedrijf?

MKB Nederland

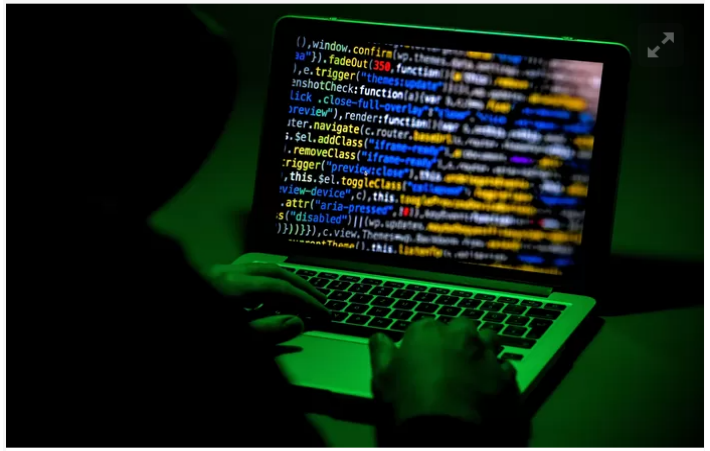
nationale nederlanden

Delen van data

Ontwikkelingen cyberrisk



Voorbeeld Ransomware (‘klantenservice’)



© EPA

Gehackte bedrijf in Helmond slechts topje van de ijsberg: ‘duizenden mkb’ers digitaal gegijzeld’

HELMOND - Twee Helmondse bedrijven zijn slachtoffer geworden van gijzelingssoftware. Een van hen betaalde losgeld om zijn door hackers platgelegde computers terug te krijgen. Ze zijn zeker niet de enige slachtoffers; daders mikken vaak op kleinere bedrijven.

Chiel Timmermans 03-08-19, 07:00 Laatste update: 14:30 Bron: ED

security.nl presented by: Certified Secure

Nieuws Achtergrond Community

Nieuws

Brabants logistiek bedrijf betaalt losgeld na infectie door Lockbit-ransomware

maandag 4 mei 2020, 09:37 door Redactie, 15 reacties

De Brabantse logistiek dienstverlener Van der Helm Logistics heeft criminelen losgeld betaald nadat bestanden door de Lockbit-ransomware waren versleuteld. De realtimeback-ups waren ook door de ransomware versleuteld en de tapestreamer voor de tapeback-ups was kapot gegaan. Dat laat het bedrijf tegenover De Volkskrant weten.

De infectie vond plaats in februari. Bestanden op twintig servers en tweehonderd pc's werden versleuteld, waaronder ook back-ups. De aanvallers wisten binnen te komen via een bruteforce-aanval op een webserver die een verouderde vpn-dienst draaide, zo laat antivirusbedrijf McAfee in een analyse van de Lockbit-ransomware weten. Via de aanval hadden de aanvallers het beheerderswachtwoord verkregen en daarmee toegang tot andere systemen in het netwerk.

"Helaas is dit geen uniek geval, systemen die aan het internet hangen horen waar mogelijk altijd over multifactorauthenticatie te beschikken", aldus de virusbestrijder, die opmerkt dat organisaties daarnaast met het principe van verminderde rechten moeten werken als het gaat om het inloggen op systemen.

Doordat de aanvallers beheerdersrechten hadden konden ze ook de back-ups van het Brabantse bedrijf versleutelen. "En de tapestreamer die back-ups regelt, was net kapot. Murphy's law: als het eenmaal fout gaat, gaat alles fout", zegt directeur Richard van der Helm tegenover De Volkskrant.

In eerste instantie wilde het bedrijf het losgeld niet betalen, laat Van der Helm weten. Het herstellen van alle getroffen systemen en het opnieuw scannen van de voorraad zou echter weken duren. "Dan konden we onze contractuele verplichtingen niet nakomen en zouden we al vrij snel richting faillissement gaan. We moesten onderhandelen", aldus de directeur die het losgeld uiteindelijk betaalde. Een exact bedrag wordt niet genoemd, maar het zou vergelijkbaar zijn met de 197.000 euro die de Universiteit Maastricht voor het ontsleutelen van bestanden betaalde.

NIEUWS GIJZELSOFTWARE

Hackers gijzelen Koninklijke Reesink – impact op bedrijf ‘enorm’

De Nederlandse landbouwdistributeur Royal Reesink is slachtoffer geworden van een aanval met gijzelsoftware. Het Apeldoornse bedrijf, dat in 10 landen vestigingen heeft en in 2019 een omzet had van bijna 1 miljard euro, lag sinds begin juni plat. Zeventig procent van de 35 aangesloten bedrijven werd geraakt door de digitale aanval.

Huib Modderkolk 11 juni 2020, 15:18

Hoeveel wordt er buitgemaakt?

Foto ter illustratie. © ANP XTRA

Gijzelsoftware kost gemeente Lochem twee ton

Bij de inbraak in het computersysteem is de gemeente Lochem in juni door het oog van de naald gekropen. De gemeente werd getroffen door gijzelsoftware. Daarbij leggen hackers beslag op belangrijke bestanden en eisen daar losgeld voor.

NIEUWS GIJZELSOFTWARE

Universiteit Maastricht betaalde hackers kwart miljoen euro

De Universiteit Maastricht (UM) heeft tussen de 200 duizend en 300 duizend euro betaald aan hackers die het universiteitssysteem met gijzelsoftware hadden vergrendeld. Het bestuur van de universiteit zag zich genoodzaakt te betalen omdat ook de back-up gekaapt was.

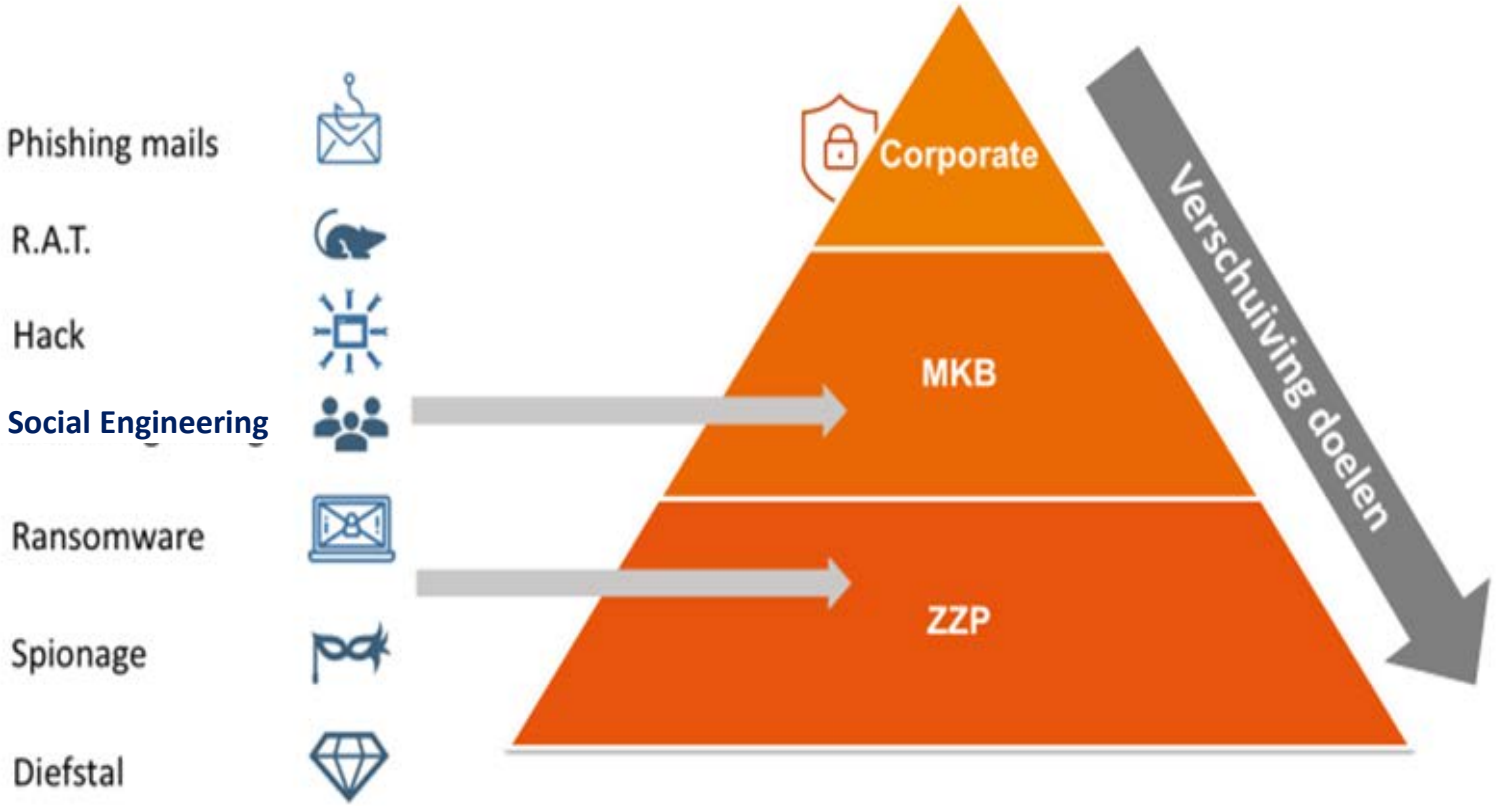
Mark Misérus en Huib Modderkolk 24 januari 2020, 5:00

MKB Nederland

nationale nederlanden

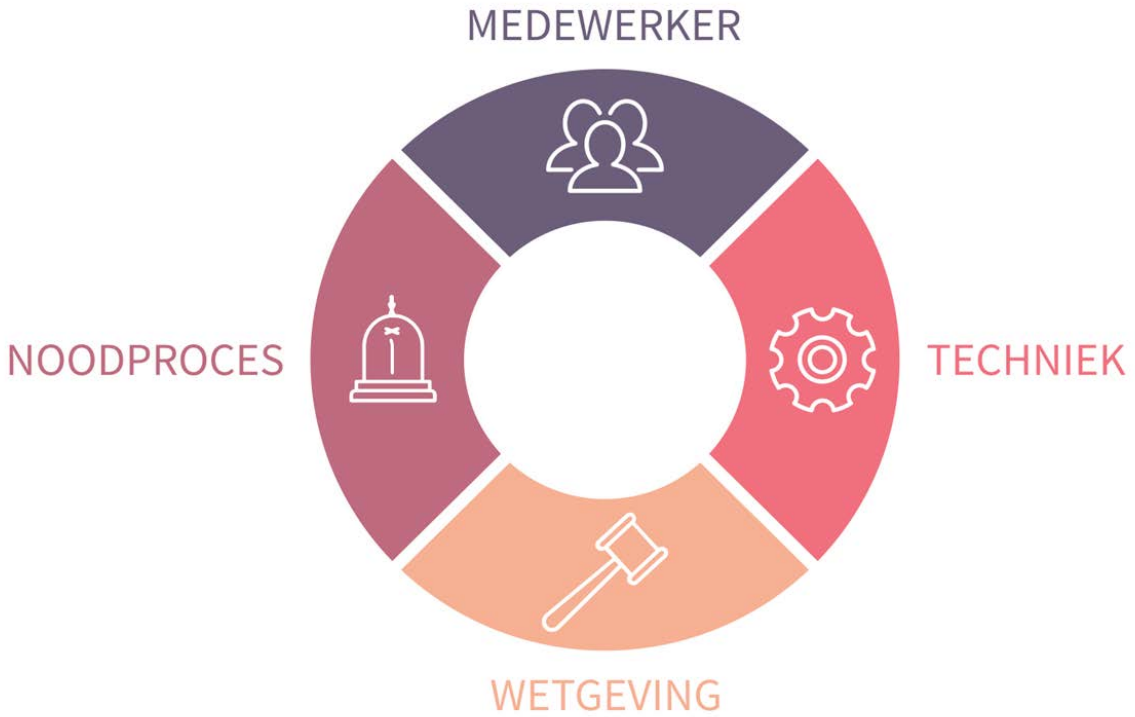
Dit is ondernemen

Ontwikkelingen cyberrisk

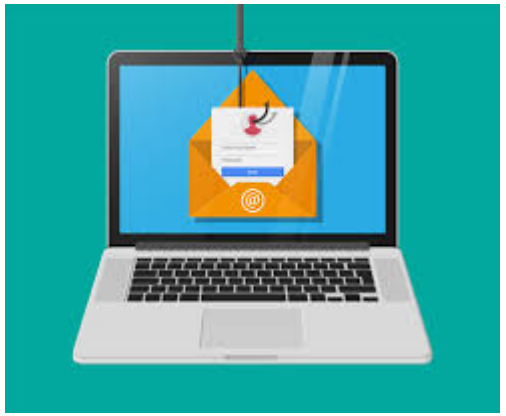


Risicogebieden

Inschatten van je risico’s



Grotere kans op een hack dan op een brand



Cyberaanval: 67%

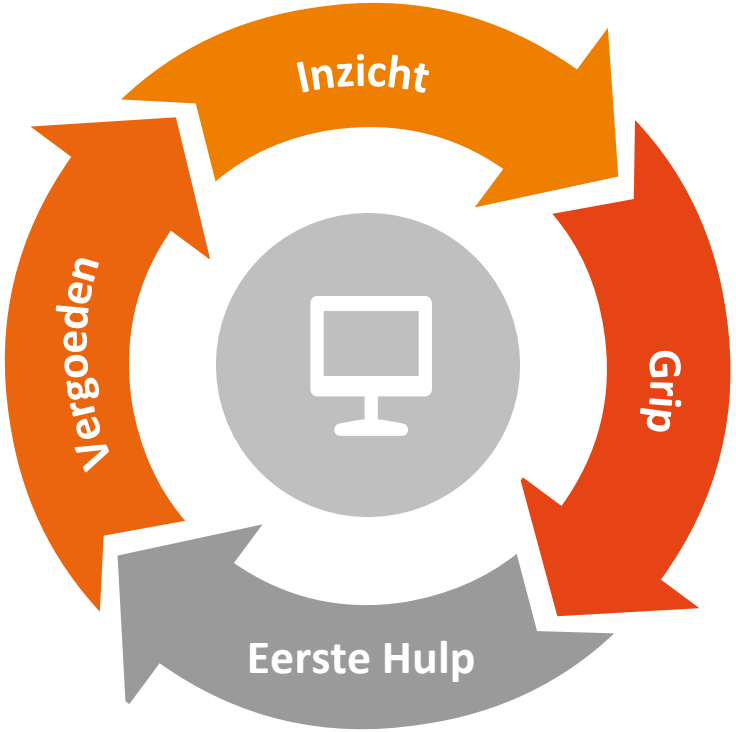
Datalek: 58%

Brand: 28%

Inbraak: 7%

100% veilig bestaat niet

We komen wel in de buurt



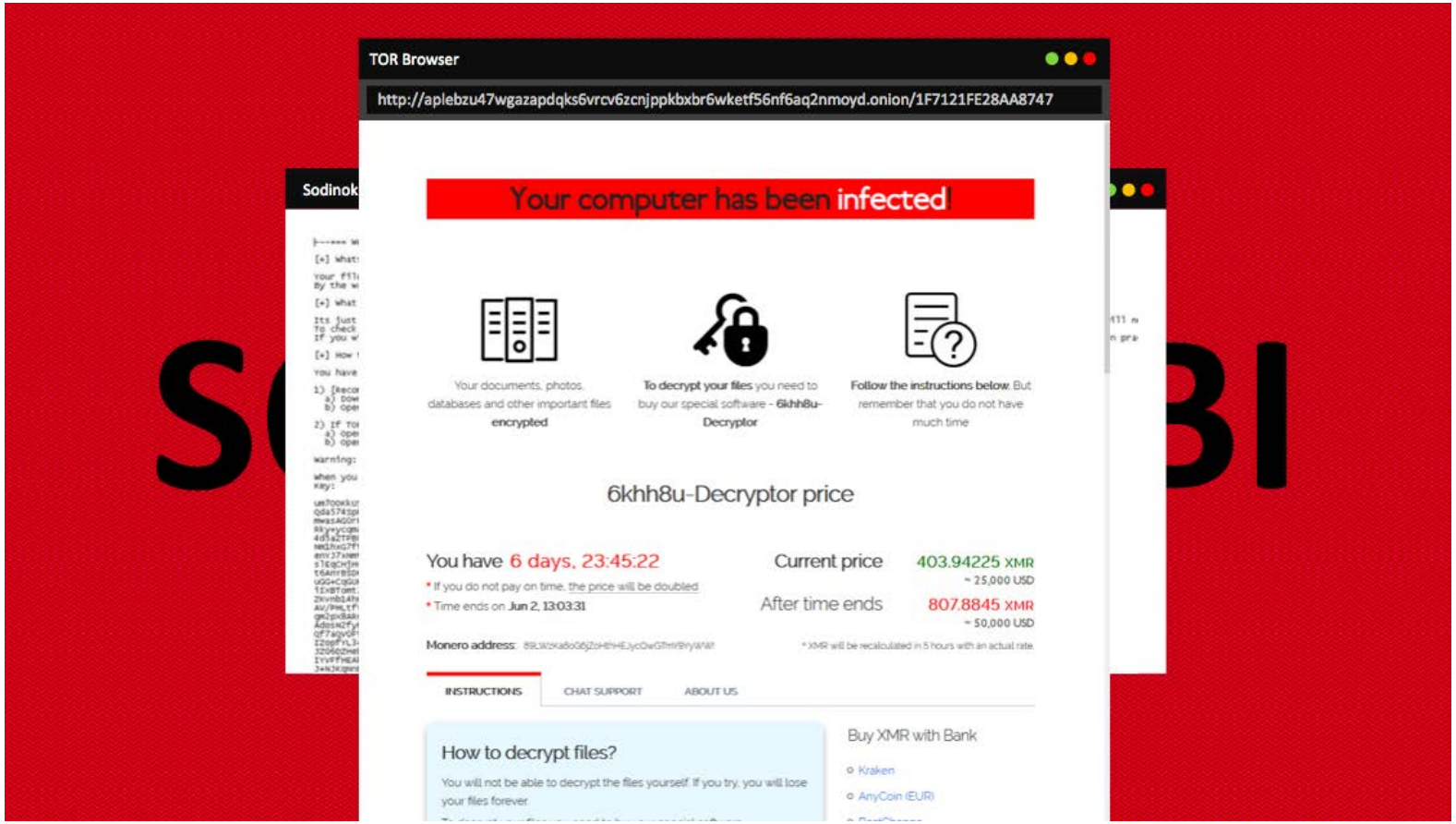
MKB Nederland

nationale nederlanden

Dit is ondernemen

Ransomware

'Sodinokibi'

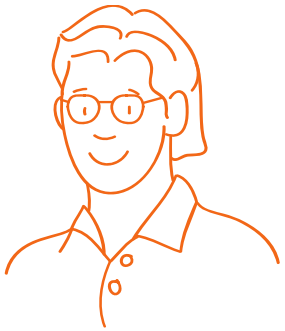


MKB Nederland

nationale nederlanden

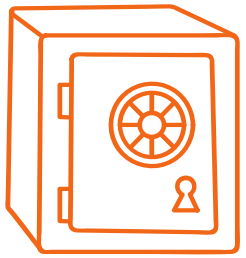
Dit is ondernemen

Veel gehoorde aannames cyberrisk

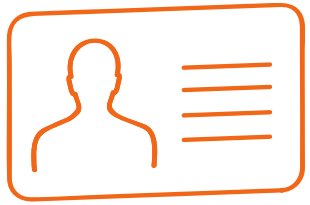


Mijn IT'er regelt dit

Alles staat in de cloud



Bij mij valt toch niets te halen



Ik bewaar / verwerk geen persoonsgegevens

Geen prioriteit

Cybercriminaliteit & MKB

Samenvatting

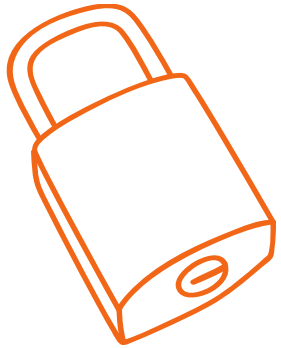
- Meest voorkomende vormen: phishing, hacking, malware, ransomware.
- Ook het MKB loopt risico: ‘Bij ons valt toch niets te halen’ is een misvatting.
- De grootste risico’s: financiële gevolgen van stilgelegd bedrijf of datalek.
- Oorzaken: zwakke wachtwoorden, achterstallige updates, geen prioriteit.
- Onwetende medewerkers zijn grootste kwetsbaarheid, maar ook 1e verdedigingslinie.

Wat zijn de gevolgen?

Altijd financiële schade door cyberincidenten

1: Bedrijfsstilstand

- Herstellen schade
- Verlies van omzet
- Kwijt raken van klanten
- Reputatieschade



2. Datalek

- Aansprakelijk worden gesteld
- Boete Autoriteit Persoonsgegevens
- Reputatieschade

Cybercriminaliteit en de gevolgen

Samenvatting

- Financiële schade
  - Eigen schade: bedrijfsstilstand, gegevensverlies, kosten voor herstel
  - Aansprakelijkheid, boete bij datalek
- Goed om te weten: niet persoonlijk bedoeld
- Wat te doen:

1. Bel het alarmnummer van je cyberverzekering / IT-partner / Cyberwacht
2. Doe aangifte

- Verzekeren van financiële schade is mogelijk

Preventie begint hier…

Uitgangspunten

- Erken dat er cyberrisico’s zijn, wees niet naïef, neem het serieus.
- Denk na over de gevolgen wanneer jouw systemen (IT/OT) niet meer werken.
- Cyber- en data security is geen project, het is een doorlopend proces.
- Het is een gezamenlijke verantwoordelijkheid dus betrek iedereen hierbij.
- Maak gemaakte fouten bespreekbaar.
- Maak cyber- en data security prioriteit; en als dit intern niet mogelijk is, besteed het uit.

10 vragen aan je IT-er

Samenvatting

1. Zijn wij goed beveiligd?
2. Wat is ons meest kwetsbare punt?
3. Welke data is het meest interessant voor criminelen en/of concurrenten?
4. Is dat onderdeel / zijn die onderdelen extra goed beveiligd?
5. Wie is verantwoordelijk voor de veiligheid van persoonsgegevens?
6. Hebben we een noodplan in geval van hack of datalek?
7. Is iedereen in het bedrijf daarvan op de hoogte?
8. Maken we backups?
9. Testen we de backups?
10. Wat zou ik vandaag nog moet regelen om de digitale veiligheid te verbeteren?

Wachtwoordbeleid

- Maak een wachtwoordbeleid, deel deze centraal, leg het uit
- Focus op lengte (geen wachtwoord maar wachtzin)
- Gebruik een wachtwoordkluis (beveilig hem met MFA)
- Niet periodiek wisselen van wachtwoorden
- Sta zwakke wachtwoorden niet toe
- Stel multi-factor in op alle extern bereikbare diensten
- Maak gebruik van notificaties van haveibeenpwnd.com

Checklist / Quick wins

- Maak een noodplan!
- Installeer goede anti-virus software en firewalls
- Zorg dat alle software up to date is, patchmanagement!
- Maak een wachtwoordprotocol
- Investeer in goede back-up faciliteiten
- Test met het terugzetten van je back-ups
- Inventariseer welke apparatuur er in je systemen hangen
- Versleutel (encrypt) alle apparaten (optie endpoint security)
- Invoeren van 2 factor authenticatie (ook intern)
- Veilige e-mail voor vertrouwelijke informatie overdracht

Cybersecurity: wat moet je doen?

Samenvatting

1. Ga in gesprek met je IT-er
2. Maak een noodplan
3. Neem preventieve maatregelen
4. Verdiep je in een cyberverzekering

En: stel een 'DHV’-er (Digital Hulp Verlener) aan

Kortom: maak cyber & data security een prioriteit!

Gratis online cyberscan:
www.nn.nl/cyberpreventie

Doe de gratis online cyberscan: hoe cyberveilig is jouw bedrijf?

- Binnen 7 minuten inzicht in de cyberrisico's
- Inzicht op 4 thema's:
  Techniek, medewerkers, wetgeving en noodplan

Start de gratis cyberscan | Lees meer

Let op: voor de cyberscan ga je naar Perfectday.nl.
Perfect Day is onafhankelijk dochter van Nationale-Nederlanden.

MKB Nederland

nationale nederlanden

Dit is ondernemen