Het aantal aanvallen blijft toenemen. Waar gaat het mis?

Cyber attacks in onze maatschappij

Whitepaper voor business- en ICT-managers

felloo

In deze whitepaper

‘De meeste aanvallen zijn ongericht en kunnen elk bedrijf raken.’

Cyber attacks in onze maatschappij

Sinds een aantal jaar is cyber security een belangrijk begrip geworden binnen onze maatschappij. De transitie naar het moderne werken, waarin er veel tijds- en plaatsonafhankelijk wordt gewerkt, heeft dit in een stroomversnelling gebracht. Het werken op meerdere plekken en devices brengt dan ook de nodige risico’s met zich mee. Echter zijn er nog te weinig ondernemers die zich bewust zijn van de risico’s die zij lopen door cyberaanvallen.

De meeste aanvallen zijn ongericht en kunnen elk bedrijf raken.

Verreweg de meeste cyberaanvallen worden uitgevoerd zonder van tevoren te kijken naar het slachtoffer. Hackers gebruiken bots om bijvoorbeeld op grote schaal phishing mails te sturen of om duizenden inlogpogingen op verschillende systemen uit te proberen. Het is schieten met hagel, maar ook daarmee tref je soms je doel. Dit zijn dan ook de aanvallen waar de meeste organisaties mee te maken krijgen. Dit soort aanvallen zijn daarom ook goed tegen te houden, mits de systemen op een juiste manier beveiligd zijn.

‘Het aantal aanvallen blijft toenemen.’

Nu wordt er weleens beweerd dat het aantal cyberaanvallen aan het afnemen is. Dit is helaas niet waar. Wat wel waar is, is dat het aantal virusaanvallen afneemt, maar malware aanvallen en phishing aanvallen nemen sterk toe. Daarbij worden de cyberbedreigingen slimmer en minder goed zichtbaar.
Het MKB is bijvoorbeeld het vaakst slachtoffer van malware en zeker 1 op de 5 van deze bedrijven wordt getroffen door cybercriminaliteit. Ondanks dit gevaar nemen ondernemers volgens de NCTV nog onvoldoende (basis) maatregelen om cybercriminelen buiten de deur te houden. Dat is een groot risico voor ondernemers, die net als de rest van de maatschappij volledig afhankelijk zijn van digitale middelen. Staat de IT stil, dan staat ook het bedrijf stil met grote problemen en kosten tot gevolg. De vraag is niet of, maar wanneer u te maken krijgt met een cyber risico.

Dit zijn de feiten...

- Sinds 2019 is cybercriminaliteit **verdrievoudigd**
- **72% van de Nederlandse** bedrijven kreeg in de laatste 12 maanden te maken met een cyberaanval
- Een groot deel van deze aanvallen vinden tegenwoordig plaats **bij kleine & middelgrote organisaties.**

← terug naar menu

NIS2-Richtlijn

In de afgelopen maanden is er veel gesproken over de nieuwe Europese Richtlijn NIS2. Je zult er ongetwijfeld iets van voorbij hebben zien komen. Maar, wat houdt het in? En wat moet je er precies mee?

NIS2 staat voor de "Tweede Richtlijn betreffende de veiligheid van netwerk- en informatiesystemen" en is een belangrijke Europese wetgeving op het gebied van cyberbeveiliging. Deze richtlijn werd opgesteld om de cyberbeveiliging in Europa te versterken en de weerbaarheid tegen cyberaanvallen te vergroten. Hier zijn enkele van de belangrijkste invloeden van NIS2 op Nederlandse organisaties:

01

Beveiligingsmaatregelen

NIS2 vereist dat beheerders van essentiële diensten en aanbieders van digitale diensten passende beveiligingsmaatregelen implementeren om de veiligheid van hun netwerk- en informatiesystemen te waarborgen.

02

Incidentmelding

Onder NIS2 moeten organisaties beveiligingsincidenten melden aan de nationale autoriteiten. Dit draagt bij aan de mogelijkheid van snelle reactie en coördinatie bij cyberaanvallen, wat de schade kan beperken.

03

Bewustwording en Cultuurverandering

NIS2 moedigt organisaties aan om een cultuur van cybersecurity en bewustwording te bevorderen. Dit vereist mogelijk bewustwordingstrainingen voor medewerkers en een grotere nadruk op cybersecurity in de bedrijfscultuur.

04

Boetes en Sancties

Organisaties die niet aan de vereisten van NIS2 voldoen, kunnen worden onderworpen aan boetes en sancties. Dit zorgt voor een stimulans om serieus werk te maken van cyberbeveiliging en naleving van de richtlijn.

05

Herzieningen en Aanpassingen

NIS2 kan in de loop van de tijd worden herzien en aangepast om bij te blijven met de veranderende cyberdreigingen en technologische ontwikkelingen. Nederlandse organisaties moeten zich bewust zijn van deze mogelijke veranderingen en hun cybersecuritystrategieën dienovereenkomstig aanpassen.

NIS2 als basis van jouw Security

In het kader van de NIS2-richtlijn komt het belang van basismaatregelen met betrekking tot cybersecurity duidelijk naar voren. Deze maatregelen vormen de basis voor een solide cybersecurity-infrastructuur en zijn cruciaal om te voldoen aan de eisen van de richtlijn.

Door deze basismaatregelen serieus te nemen en te implementeren, kunnen organisaties niet alleen voldoen aan de voorschriften van NIS2, maar ook hun digitale weerbaarheid vergroten en de potentiële impact van cyberaanvallen verminderen. Dit is van essentieel belang om te voldoen aan de verplichtingen van NIS2 en de algehele cyberveiligheid te verbeteren, wat van vitaal belang is in het moderne digitale landschap.

Waar gaat het mis?

De 8 cruciale punten voor een betere security

felloo

01 Multifactor Authenticatie is niet ingesteld

Wachtwoorden zijn vaak nog steeds de sleutel tot alles. Dat brengt risico's met zich mee. Een groot deel van de datalekken wordt namelijk veroorzaakt door eenvoudig te kraken wachtwoorden. Sterker nog, als je voor veiligheid van een cloud omgeving volledig moet vertrouwen op een zwak wachtwoord als 'welkom01' is het niet de vraag of je gehackt wordt maar enkel nog wanneer. De kans is overigens groot dat dit dan al is gebeurd, zonder dat je het door hebt gehad. Tegenwoordig is het advies om wachtwoorden niet meer periodiek te wijzigen, maar te werken met 1 sterk wachtwoord aangevuld met Multi-Factor authenticatie (MFA).

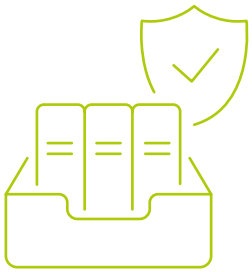
02 Geen back-up

Een back-up is misschien wel de belangrijkste maatregel die genomen dient te worden. Een omgeving is namelijk nooit voor 100% te beveiligen. Je laatste redmiddel is dan een back-up. Deze zorgt ervoor dat alle bedrijfsdata op een offsite locatie staat opgeslagen, waardoor je in geval van nood deze weer kunt terugzetten.

03 Geen antivirus

Tegenwoordig is een antivirus een van de standaard toepassingen voor het hanteren van een veilige werkplek. Echter komt het nog steeds voor dat organisaties geen antivirus geactiveerd hebben op de werkplekken. Hierdoor krijgen schadelijke software en virussen vrij spel.

04 Niet (regelmatig) laten testen



Vaak wordt er gedacht: "Zodra er niks gebeurd, loopt ik geen risico." Dit is helaas niet het geval. Cybersecurity is een continue proces en daarom is het belangrijk om constant in ontwikkeling te zijn. Het beste is om periodiek een pentest uit te voeren of een vulnerability scan te draaien zodat je nooit voor onverwachte verassingen komt te staan. Wat nu veilig is, kan morgen weer onveilig zijn. En ook de wet- en regelgeving rondom privacy en informatiebeveiliging verandert continu. Tegelijkertijd wordt cybercriminaliteit steeds geavanceerder. Het is dus belangrijk om continu scherp te blijven en je goed te (blijven) wapenen tegen deze criminaliteit. Als je dit niet doet, kunnen de gevolgen voor jouw bedrijf immens zijn. Denk aan datalekken, imagoschade en zelfs faillissement. Kortom, voorkomen dus!

05 Onveilige apparaten

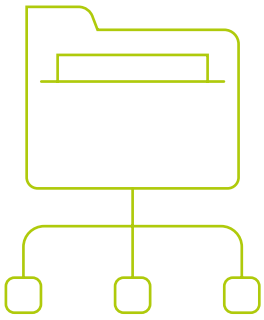
Mobiel werken is in de huidige maatschappij een normale zaak geworden. Echter brengt dit wel de nodige risico's met zich mee. Denk aan laptops en smartphones die onderweg gestolen worden of vergeten worden. Soms zijn die niet of niet afdoende beveiligd en heeft de dief of vinder vrij spel. Maak van je mobiele apparaten geen beveiligingsrisico en implementeer een Mobile Device Management (MDM) beleid binnen jouw organisatie.

06 Geen e-mailfiltering

E-mail blijft nog altijd een van de meest gebruikte systemen voor cybercriminelen. We hebben allemaal wel eens te maken gehad met phishingmails. Nog steeds is het zo dat 90% van de malwarebesmettingen plaatsvind door e-mailing. Phishing gebeurt tegenwoordig op veel verschillende manieren, maar bij veel organisaties wordt er nog niet met een geavanceerde e-mailfilter gewerkt.

Een steeds vaker voorkomend beschermingsmechanisme is e-mail sandboxing. Dit is een beveiligingsfunctie die helpt bij het identificeren en blokkeren van deze nieuwe bedreigingen, vaak zero-day- of zero-hour-bedreigingen genoemd. Een sandbox is een geïsoleerde testomgeving waar bestanden veilig kunnen worden geopend zonder enige schade aan te richten.

07 Geen goede rechtenverdeling



Bij veel organisaties is er nog geen concreet beleid over een rechten- en rollenverdeling. Hierdoor kan hij bijvoorbeeld zijn dat een administratiemedewerker bij directiemappen kan. Daarnaast zien we nog veel dat bij het aanmaken van nieuwe gebruikers het profiel van oude gebruikers wordt gebruikt. Dit kan ertoe leiden dat personen toegang krijgen tot zaken waar dat niet zou moeten. Hetzelfde geldt voor het afschalen van gebruikers. Vaak is hier geen duidelijke procedure voor. Wenselijk is om dergelijke processen te automatiseren zodat hier geen calamiteiten ontstaan.

08

Ongetraind personeel

Ook al is jouw IT-omgeving nog zo goed beveiligd, de menselijke factor blijft altijd een risico. Een fout is dan ook snel gemaakt. Er wordt namelijk toch nog vaak op een onveilige link geklikt. Daarnaast zien we ook nog regelmatig post-its met wachtwoorden op monitors of in notitieblokjes. Bewustwording m.b.t. digitale veiligheid is een niet te onderschatten item in de huidige maatschappij. Train je personeel hierin en maak beleid over zaken als wachtwoorden, webfiltering, USB-sticks en het locken van schermen.

Maak jouw security inzichtelijk met de CyberVeilig-Check!

Om Nederlandse organisaties te helpen heeft het Nederlandse Digital Trust Center een CyberVeilig-check opgesteld. Het Nederlandse Digital Trust Center (DTC) heeft als doel om ondernemers en organisaties te ondersteunen bij het verbeteren van hun cybersecurity. De CyberVeilig check is een van de diensten. Deze check is bedoeld om organisaties te helpen hun digitale weerbaarheid te verbeteren en potentiële zwakke plekken in hun cybersecurity te identificeren.

CyberVeilig Check voor ZZP en MKB

Ga naar www.digitaltrustcenter.nl en doe de check

Na het invullen van de vragenlijst wordt er een adviesrapport gegenereerd dat is afgestemd op de antwoorden van de organisatie. Dit rapport bevat aanbevelingen en actiepunten om de cybersecurity te verbeteren op basis van de beoordeling van de organisatie. Het kan ook links bevatten naar hulpmiddelen en informatiebronnen die de organisatie kan gebruiken om aanbevolen verbeteringen door te voeren.

Meer weten over security binnen het MKB?

Wij denken graag met je mee!

De meeste mkb-bedrijven kunnen niet meer zonder digitale werkplekken. Daarom is het essentieel dat deze goed beschermd zijn tegen cybercrime, menselijke fouten en calamiteiten. Zorg ervoor dat cybercrime je zaken niet in de war schopt, beveilig je hardware en dataverkeer goed en vergeet niet je personeel op de hoogte te houden.

Plan een afspraak of een call met ons in als we jou verder kunnen helpen met security of kunnen helpen om te zorgen dat jouw organisatie altijd, en overal, vanaf ieder device op een veilige manier kan werken!

felloo

Jouw cybersecurity goed geregeld met Felloo

Over onze whitepapers

Onze experts publiceren regelmatig whitepapers waarin je onze visie terugvindt op actuele onderwerpen. Vaak gaan deze over ICT-thema's of over thema's die daaraan raken, zoals security, digitalisering en cloud-ontwikkelingen. Deze whitepapers maken we om onze ervaring en expertise met jou te delen. Om je te inspireren en te laten zien wat er tegenwoordig allemaal mogelijk is. Ben je aan de hand van dit of een ander whitepaper geïnteresseerd geraakt in ons en onze diensten? Neem dan contact op met jouw accountmanager of ga naar www.felloo.nl.

088 200 2400
info@felloo.nl

Felloo B.V.
Twentepoort Oost 22
7609 RG Almelo

CHALLENGE THE CLOUD