<HET DIGITALE KOMPAS>

</DE ZIN EN ONZIN VAN CYBERSECURITY>



#1

<BRANDARIS>

</CYBERSECURITY>

<BRANDARIS CYBERSECURITY B.V.>
Kalkovensweg 6b
1815 KZ Alkmaar

+31 (0)72 202 97 95
info@brandaris.it
www.brandaris.it

<KVK> 94696675
<BTW> NL866862833B01
<IBAN> NL58REVO7619561102
<BIC> REVONL22



<INHOUDSOPGAVE>

02 </INLEIDING>

03 </DE GROOTSTE MISVERSTANDEN OVER CYBERSECURITY>

05 </WAT CYBERCRIMINELEN ÉCHT WILLEN>

07 </RANSOMWARE: HOE CRIMINELEN JE BEDRIJF DIGITAAL GIJZELEN>

08 </PHISHING: DE ZWAKSTE SCHAKEL IS EEN MENS>

13 </CYBERSECURITY ZONDER GEDOE: 5 ACTIES DIE ÉCHT WERKEN>

18 </CHECKLIST>

20 </TOT SLOT>

21 </BONUSFABELS>

</INLEIDING>

<CYBERSECURITY>
DE ZIN EN ONZIN VAN CYBERSECURITY

Cybersecurity. Iedereen heeft het erover, maar weinigen begrijpen écht wat belangrijk is en wat niet. Moet je bang zijn voor hackers in een hoodie? Is een firewall genoeg? Hoe groot is de kans dat jouw bedrijf wordt getroffen? En vooral: wat moet je nu werkelijk doen om je onderneming te beschermen zonder dat het je fortuinen kost of je bedrijf tijdelijk stillegt?

De waarheid is: veel adviezen over cybersecurity zijn óf te technisch óf gebaseerd op doemscenario's die weinig met de praktijk te maken hebben, óf simpelweg verouderd. Veel zogenaamde 'best practices' waren ooit nuttig, maar werken niet meer in de realiteit van vandaag.

Cybercrime is al lang geen ver-van-je-bed-show meer. Grote bedrijven halen het nieuws, maar ondertussen zijn het vooral mkb'ers die slachtoffer worden — gewoon omdat ze 'makkelijk' zijn voor cybercriminelen, doordat ze niet goed voorbereid zijn. Daarom dit boek. Geen ingewikkeld IT-jargon of gladde verkooppraatjes, maar een nuchtere, praktische gids over wat wél en niet nodig is.

<CYBERSECURITY>
FEITEN VS. FICTIE

In de media lees je over datalekken, ransomware-aanvallen en miljoenenboetes voor bedrijven die hun beveiliging niet op orde hebben. Maar je leest minder over de kleine bedrijven die geruisloos worden leeggetrokken, over zzp'ers die na een phishing-aanval zonder klantenbestand zitten, of over de bakker op de hoek die geen pinbetalingen meer kan accepteren omdat zijn systeem is gegijzeld.

Het is gebaseerd op meer dan 30 jaar collectieve ervaring in het beschermen van bedrijven — van kleine ondernemingen tot grote organisaties. Wij weten wat werkt en wat niet.

Het goede nieuws? Met de juiste basismaatregelen kun je 80% van de aanvallen eenvoudig voorkomen.

Of je nu directeur bent, IT-verantwoordelijke of gewoon iemand die zich afvraagt of het met die wachtwoorden en phishing-mails wel goed zit: deze gids helpt je op weg.

</DE GROOTSTE MISVERSTANDEN OVER CYBERSECURITY>

Cybersecurity heeft een imagoprobleem. Voor de één is het een technisch hoofdpijndossier, voor de ander een ver-van-mijn-bed-show. Maar wat het écht is? Een noodzakelijk onderdeel van je bedrijfsvoering net zoals je verzekeringen, administratie en personeelsbeleid.

Toch blijven er hardnekkige misverstanden rondzwerven die ervoor zorgen dat veel mkb'ers onbeschermd zijn. Dit zijn de gevaarlijkste:

<MISVERSTANDEN>
"WIJ ZIJN TE KLEIN VOOR HACKERS"

Dit is misschien wel het meest gehoorde argument — en het meest risicovolle. Cybercriminelen maken geen onderscheid op basis van bedrijfsgrootte. Ze gaan voor de makkelijkste prooi.

Feit: De meeste cyberaanvallen zijn niet gericht op een specifiek bedrijf, maar op willekeurige organisaties. Hackers gebruiken bots die automatisch zwakke plekken scannen en aanvallen zodra ze een kans zien. Of je nu een mkb'er met 10 medewerkers bent of een multinational, als je een lek hebt, word je gevonden.

Gevolg: Juist kleine bedrijven worden vaak slachtoffer, omdat ze hun beveiliging niet op orde hebben. Ze zijn de digitale versie van een huis zonder slot op de deur. Of ze zijn de opstap naar jouw prestigieuze klanten.

<MISVERSTANDEN>
"ONZE IT'ER REGELT HET WEL"

Ja, een goede IT'er is belangrijk. Maar cybersecurity is geen taak voor één persoon — het is een verantwoordelijkheid van de hele organisatie. Ook is het maar de vraag of je contract uit 2001 een clausule heeft voor cybersecurity of dat het toch stiekem jullie eigen verantwoordelijkheid is.

Feit: De meeste succesvolle hacks gebeuren niet door technische zwakheden, maar door menselijke fouten. Denk aan medewerkers die zwakke wachtwoorden gebruiken, op phishinglinks klikken of gevoelige data naar privé-mail sturen. De kwetsbare systemen zijn daarna vooral een makkelijk doelwit.

Gevolg: IT kan systemen up-to-date houden, maar als de rest van de organisatie niet meewerkt, is dat dweilen met de kraan open.



<MISVERSTANDEN>

“CYBERSECURITY IS TE DUUR EN TE INGEWIKKELD”

Dit is een veelgehoord argument, maar het klopt niet. De meeste cyberaanvallen hadden met eenvoudige en goedkope maatregelen voorkomen kunnen worden.

Feit: Een wachtwoordmanager, tweefactorauthenticatie en regelmatig updaten van software kosten vrijwel niets, maar maken al een enorm verschil.

Gevolg: De kosten van een cyberaanval — zoals omzetverlies, boetes en reputatieschade — zijn altijd hoger dan de investering in preventie.

</WAT CYBERCRIMINELEN ÉCHT WILLEN>

Cybercriminelen zijn geen eenzame hackers in hoodies die nachtenlang code typen. In werkelijkheid zijn het georganiseerde bendes, soms met honderden medewerkers, duidelijke verdienmodellen en zelfs een klantenservice. Cybercrime is big business. Voor jou als ondernemer is het belangrijk om te snappen hoe ze werken. Want als je weet wat cybercriminelen willen, weet je ook hoe je het ze moeilijker kunt maken.

<DATA IS GELD>

WAAROM JOUW GEGEVENS GOUD WAARD ZIJN

Jouw bedrijfsgegevens lijken misschien niet bijzonder, maar voor cybercriminelen zijn ze goud waard. Zelfs de simpelste informatie kan doorverkocht worden, met grote gevolgen voor jou en jouw organisatie.

Stel je voor: een hacker weet in te breken in je systeem en steelt een lijst met klantgegevens en wachtwoorden. Wat gebeurt er vervolgens? Die data belandt op het dark web, waar andere criminelen ze kopen om in te loggen op accounts, facturen te onderscheppen of nog meer bedrijfsnetwerken binnen te dringen. Voor jou betekent dat niet alleen een AVG-boete en boze klanten, maar ook een flinke deuk in je reputatie. Want wie wil nog met je samenwerken als hun gegevens bij jou niet veilig zijn?

Of neem het scenario waarin een hacker met jouw bedrijfsgegevens identiteitsfraude pleegt. Ineens blijken er op jouw naam bestellingen te zijn geplaatst, contracten te zijn afgesloten of zelfs leningen te zijn aangegaan. Leveranciers kloppen bij jou aan voor betalingen die jij nooit hebt goedgekeurd. In het ergste geval ontdek je pas te laat dat iemand zich als jouw bedrijf heeft voorgedaan en schade heeft aangericht dat maanden kost om recht te zetten.

Soms gebruiken criminelen jouw netwerk niet eens zelf, maar verkopen ze de toegang door aan anderen. Een onbekende partij neemt jouw IT-omgeving over en voor je het weet, ligt je hele bedrijf stil door een ransomware-aanval. Je bestanden zijn versleuteld, en als je geen back-up hebt, sta je voor een onmogelijke keuze: losgeld betalen of alles kwijtraken. Ondertussen loopt je bedrijf enorme vertraging op en lopen klanten weg omdat ze niet op jou kunnen wachten.

En dan is er nog een minder zichtbare, maar net zo schadelijke dreiging: jouw e-mailserver wordt misbruikt voor phishing en spam. Zonder dat je het weet, worden duizenden frauduleuze mails vanuit jouw naam verstuurd. Klanten en partners krijgen nepverzoeken om betalingen over te maken, en zodra ze doorhebben dat jij het niet bent, is de schade al gedaan. Niet alleen verliezen zij mogelijk geld, maar ook jij verliest hun vertrouwen. Bovendien belandt jouw e-mailadres op een zwarte lijst, waardoor zelfs jouw legitieme berichten worden geblokkeerd.

Dit zijn geen verzonnen horrorverhalen — ze gebeuren dagelijks, ook bij kleine en middelgrote bedrijven. Cybercriminelen richten zich niet alleen op grote organisaties, maar juist op bedrijven waarvan ze verwachten dat de beveiliging minder sterk is. Denk dus niet dat jouw gegevens niet belangrijk zijn. Voor de verkeerde mensen zijn ze precies dát.

</CYBERSECURITY IS GEEN LUXE>

Het is een noodzaak.

Door je beveiliging op orde te hebben, voorkom je financiële schade, juridische problemen en reputatieverlies. Want herstellen na een cyberaanval is altijd duurder dan voorkomen.

</RANSOMWARE: HOE CRIMINELEN JE BEDRIJF DIGITAAL GIJZELEN>

Stel je voor: het is maandagochtend en je opent je laptop om de week te beginnen.
Maar in plaats van je vertrouwde werkomgeving verschijnt er een verontrustend bericht op je scherm:
“Al je bestanden zijn versleuteld. Betaal €50.000 in Bitcoin, anders blijft alles onbruikbaar.”
Je klikt rond, probeert bestanden te openen, maar niets werkt. Jouw hele bedrijf ligt stil.

<RANSOMWARE>
HOE IS DIT GEBEURD?

De aanval begon misschien onschuldig. Misschien klikte een medewerker vorige week op een e-mail die eruitzag als een factuur van een leverancier. Of iemand bezocht een gehackte website zonder het te weten. Binnen enkele seconden installeerde zich ongemerkt een virus dat zich als een lopend vuurtje door je netwerk verspreidde.

Op de achtergrond deden de criminelen hun werk. Eerst versleutelden ze je bestanden, waardoor je geen toegang meer hebt tot klantgegevens, offertes en financiële administratie. Misschien hebben ze zelfs je back-ups besmet, waardoor herstellen geen optie meer is. Sommige hackers gaan nog een stap verder: in plaats van alleen je bestanden te versleutelen, stelen ze je gevoelige data. Denk aan klantinformatie, personeelsdossiers en contracten.

En dan komt de echte dreiging. Betaal je het losgeld niet? Dan dreigen ze je gegevens openbaar te maken. Klanten kunnen hun persoonsgegevens op het dark web terugvinden, concurrenten krijgen inzicht in je bedrijfsstrategieën, en je bedrijf loopt onherstelbare reputatieschade op.

<DENK NIET>
“IK HEB EEN BACKUP DUS BEN VEILIG”

Ransomware-aanvallen zijn slimmer dan dat. Criminelen weten dat bedrijven back-ups maken en proberen deze óók te versleutelen of onbruikbaar te maken. Zonder een sterk beveiligingsplan, inclusief preventieve maatregelen en regelmatige back-upcontroles, ben je kwetsbaar.

</CYBERCRIMINELEN SPELEN GEEN SPELLETJE RANSOMWARE KAN JE BEDRIJF LETTERLIJK GIJZELEN>

</PHISHING: DE ZWAKSTE SCHAKEL IS EEN MENS>

Veel ondernemers denken dat een cyberaanval begint met een zwakke plek in de software. Maar in de praktijk is technologie zelden het echte probleem. De meeste aanvallen slagen omdat iemand in het bedrijf een verkeerde beslissing neemt — en dat kan iedereen overkomen.

Stel je voor, je krijgt een e-mail van je bank met een dringende melding.:“Er is verdachte activiteit op je rekening, klik hier om je account te beveiligen.” Alles ziet er vertrouwd uit — het logo, de afzender, zelfs de toon. Zonder lang na te denken klik je op de link en log je in. Wat je niet weet, is dat je net jouw inloggegevens hebt doorgestuurd naar criminelen. Binnen minuten nemen ze je account over, onderscheppen facturen of maken geld over zonder dat je het doorhebt.

Of misschien gaat het subtieler. Je telefoon gaat: “Goedemiddag, u spreekt met IT-support. We zien een probleem met uw e-mailaccount en moeten even uw wachtwoord resetten. Kunt u dat even bevestigen?” De stem klinkt professioneel en behulpzaam. Je denkt geen moment aan fraude en geeft de informatie. Maar aan de andere kant van de lijn zit geen collega, maar een oplichter die nu toegang heeft tot je zakelijke e-mails, klantgegevens en vertrouwelijke documenten.

Soms komt de aanval zelfs via WhatsApp. De ‘directeur’ stuurt een bericht: “Ik zit in een meeting en kan niet bellen, maar we moeten dringend een betaling doen. Kun jij dit even afhandelen?” De tijdsdruk en autoriteit werken perfect — zonder verder te twijfelen wordt de betaling gedaan. Later blijkt dat de directeur hier niets vanaf weet en dat het geld verdwenen is.

Dit zijn geen extreme scenario’s, dit gebeurt dagelijks. Cybercriminelen hebben geen geavanceerde hacks nodig als medewerkers zélf de deur voor hen openzetten. Zelfs het beste beveiligingssysteem houdt geen stand als iemand binnen het bedrijf per ongeluk de sleutels weggeeft.

<PHISHING>

BEWUSTWORDING IS NET ZO BELANGRIJK ALS TECHNOLOGIE

We denken vaak dat we phishingmails wel herkennen, dat we nooit zomaar ons wachtwoord geven of een verdachte betaling doen. Maar hackers weten precies hoe ze ons moeten manipuleren. Ze spelen in op stress, tijdsdruk en routine. Elk moment kan iemand in de organisatie een kwetsbare plek zijn.

Goede cybersecurity begint daarom niet alleen met de juiste technische maatregelen, maar met gedragsverandering. Regelmatige training en bewustwording zijn essentieel om de achilleshiel van elke organisatie — de menselijke factor — te verstevigen. Want de realiteit is: zelfs goedgetrainde mensen trappen er soms nog in. Cybercriminelen blijven hun technieken verfijnen, en alleen bedrijven die hun medewerkers écht voorbereiden, blijven hen een stap voor.

<PHISHING>

CYBERCRIME IS EEN VERDIENMODEL

Hackers zijn geen hobbyisten die willekeurig bedrijven aanvallen. Cybercriminaliteit is een miljoenenbusiness, en aanvallers gebruiken geautomatiseerde tools om zwakke plekken te vinden. Ze hoeven jou niet persoonlijk te kennen — ze hoeven alleen een moment te vinden waarop je even niet oplet.



PRAKTIJKVOORBEELD JANSEN & CO >

Het was een gewone maandagochtend bij Jansen & Co, een middelgroot handelsbedrijf in bouwmaterialen.

De medewerkers begonnen hun week met de gebruikelijke routine: e-mails checken, orders verwerken en klanten te woord staan. Niemand vermoedde dat er op dat moment een cybercrimineel bezig was hun bedrijf binnen te dringen.

<FASE 1>
DE EERSTE INFILTRATIE

In een anoniem kantoor, ergens ter wereld, had een hacker een lijst met e-mailadressen van medewerkers van Jansen & Co bemachtigd. Hij stuurde een overtuigende phishingmail naar Karen, de administratief medewerkster. De e-mail leek afkomstig van een vertrouwde leverancier en bevatte een link naar een zogenaamd belangrijk document. Karen, druk bezig met haar werkzaamheden, klikte zonder argwaan op de link en voerde haar inloggegevens in op de nagemaakte website. Hiermee gaf ze de hacker toegang tot haar zakelijke e-mailaccount.

<FASE 2>
ONOPGEMERKT VERKENNEN

Met toegang tot Karens e-mail begon de hacker geduldig de omgeving van Jansen & Co te verkennen. Hij las e-mailconversaties, bestudeerde facturen en verzamelde informatie over de leveranciers en klanten van het bedrijf. Deze fase, waarin de aanvaller zoveel mogelijk informatie verzamelt zonder ontdekt te worden, kan weken tot maanden duren. Cybercriminelen blijven vaak onopgemerkt terwijl ze waardevolle gegevens verzamelen.

<FASE 3>
MANIPULATIE VAN FACTUREN

De hacker ontdekte dat Jansen & Co regelmatig betalingen ontving van diverse klanten. Hij besloot deze informatie te misbruiken door zich voor te doen als Karen en stuurde e-mails naar meerdere klanten met het verzoek toekomstige betalingen over te maken naar een nieuw bankrekeningnummer, zogenaamd om administratieve redenen. Hij voegde overtuigende kopieën van openstaande facturen bij om de geloofwaardigheid te vergroten. Deze vorm van oplichting, waarbij criminelen betalingen omleiden door zich voor te doen als een vertrouwde partij, staat bekend als factuurfraude.

<FASE 4>
ONTDEKKING EN SCHADEBEPERKING

Enkele weken later ontving de financiële afdeling van Jansen & Co meldingen van klanten die bevestiging zochten over het nieuwe bankrekeningnummer. Dit wekte argwaan, en na intern onderzoek ontdekte het bedrijf dat meerdere betalingen waren overgemaakt naar de rekening van de hacker. De totale schade bedroeg tienduizenden euro's.

</CYBERSECURITY ZONDER GEDOE: 5 ACTIES DIE ÉCHT WERKEN>

<ACTIE1>

VEILIG OMGAAN MET INLOGGEGEVENS EN JE ONLINE IDENTITEIT

Een wachtwoord alleen is geen beveiliging meer. Cybercriminelen hebben toegang tot miljarden gestolen wachtwoorden en gebruiken geautomatiseerde scripts om inloggegevens te testen op andere platforms. Veel bedrijven maken het hen onbedoeld veel te makkelijk.

WAT JE MOET DOEN:

- **Tweefactorauthenticatie (2FA)** verplichten op alle belangrijke accounts (e-mail, boekhouding, CRM, cloudopslag). Dit voorkomt dat een gestolen wachtwoord direct toegang geeft tot je systemen. Als je oplossing al Passkeys ondersteunt is dit nog beter!
- **Een wachtwoordmanager** gebruiken om unieke en sterke wachtwoorden automatisch te genereren en op te slaan. Dit voorkomt hergebruik en zwakke wachtwoorden. Zelfs een wachtwoordenboekje is al beter dan overal hetzelfde wachtwoord.
- **Argwanend denken**, standaard wantrouwen en altijd verificatie eisen voordat toegang wordt verleend. Niet alleen voor medewerkers, maar ook voor leveranciers en externe partijen die toegang hebben tot je systemen.

WAAROM?

Cybercriminelen richten zich niet op één zwakke plek, maar op een combinatie van slechte gewoonten. Een hergebruikt wachtwoord, een onbeveiligde e-mail en het ontbreken van 2FA is voor hen een open deur. back-ups maken en proberen deze óók te versleutelen of onbruikbaar te maken. Zonder een sterk beveiligingsplan, inclusief preventieve maatregelen en regelmatige back-upcontroles, ben je kwetsbaar.



<ACTIE2>

BACK-UPS: ZORG DAT JE EEN PLAN B HEBT

Een back-up is geen back-up als je hem niet kunt terugzetten. Toch komen veel bedrijven daar pas achter als het te laat is.

WAT JE MOET DOEN:

- **Automatische back-ups instellen** van alle essentiële systemen en bestanden.
- **Een offline back-up bewaren** die losstaat van je netwerk (zodat ransomware hem niet kan versleutelen).
- **Regelmatig testen of je back-up werkt** en of je hem daadwerkelijk kunt herstellen.
- **Versleutelde back-ups maken**, zodat ze niet door onbevoegden kunnen worden uitgelezen.

WAAROM?

Ransomware versleutelt je bestanden en criminelen eisen losgeld om ze terug te geven. Als je een recente en veilige back-up hebt, kun je de aanval afslaan zonder te betalen. Het voorkomt helaas alleen niet de eventuele afpersing.

<ACTIE3>

UPDATES EN PATCHES: SLUIT DE ACHTERDEUR

Cybercriminelen zoeken continu naar bedrijven die verouderde software gebruiken. Een niet-gepatchte kwetsbaarheid in een systeem is voor hen net een openstaande achterdeur deur in jouw huis. Als ze zo je huis kunnen binnensluipen, misbruiken ze zo'n buitenkans graag om terecht te komen in de kamer waar de kluis verborgen is.

WAT JE MOET DOEN:

- **Automatische updates inschakelen voor alle software en apparaten.**
- **Geen 'end-of-life' software gebruiken** zoals oude versies van Windows of verouderde versies van applicaties zoals Google Chrome of Acrobat Reader.
- **Beheer alle software en apparaten die in gebruik zijn** binnen je organisatie, zodat niets onbeschermd blijft.

WAAROM?

De meeste cyberaanvallen maken misbruik van bekende kwetsbaarheden waarvoor allang een oplossing bestaat. Toch worden deze updates vaak maandenlang uitgesteld.

<ACTIE4>

ADEQUATE E-MAILBEVEILIGING: BESCHERM INKOMENDE ÉN UITGAANDE COMMUNICATIE

E-mail is nog altijd het belangrijkste aanvalskanaal voor cybercriminelen. Maar het risico beperkt zich niet alleen tot wat binnenkomt ook uitgaande e-mails kunnen een risico vormen, als criminelen je domeinnaam misbruiken en je reputatie schaden.

WAT JE MOET DOEN:

- **SPF, DKIM en DMARC instellen** om te voorkomen dat criminelen valse e-mails namens jouw bedrijf kunnen versturen. (Sorry, toch technische termen, maar het is echt belangrijk.)
- **Inkomende e-mails automatisch scannen op verdachte bijlagen en links.**
- **Medewerkers trainen om verdachte e-mails te herkennen**, en niet alleen focussen op phishing. Denk ook aan CEO-fraude en factuurfraude. E-mails structureel met aandacht behandelen voorkomt heel veel ellende.

WAAROM?

Als een hacker namens jouw bedrijf phishingmails verstuurt, schaadt dat niet alleen je klanten, maar ook je reputatie. E-mailbeveiliging gaat verder dan alleen spamfilters en phishingtrainingen.

<ACTIE5>

GEDRAGSVERANDERING: CYBERSECURITY ALS DAGELIJKSE GEWOONTE

De menselijke factor is en blijft een beïnvloedbare schakel in cybersecurity. Maar gedragsverandering bereik je niet met een eenmalige training of een jaarlijkse phishingtest. Aandacht voor digitale veiligheid moet een dagelijkse gewoonte worden.

WAT JE MOET DOEN:

- **Digitale veiligheid onderdeel maken van de bedrijfscultuur** — niet iets dat 'IT regelt'.
- **Medewerkers actief betrekken** bij cybersecurity en hen verantwoordelijk maken voor veilig gedrag.
- **Een 'blame-free' meldcultuur creëren**, zodat medewerkers verdachte situaties direct durven te melden zonder angst voor straf.
- **Continu herhalen en oefenen**, bijvoorbeeld met periodieke security checks en realistische scenario's.

WAAROM?

Gedragsverandering werkt pas als veilige keuzes de standaard worden. Cybersecurity is geen IT-probleem, maar een organisatiebreed thema.



</CONCLUSIE CYBERSECURITY HOEFT NIET MOEILIJK TE ZIJN>

Veel bedrijven zien cybersecurity als een complex en duur probleem.

Maar als je je richt op deze vijf fundamentele acties, ben je al 80% veiliger dan de meeste bedrijven.

Je hoeft geen expert te zijn.
Je moet alleen zorgen dat je de basis goed op orde hebt.



</CHECKLIST: HOE VEILIG IS JOUW BEDRIJF?>

Je hebt nu een goed beeld van hoe cybercriminelen te werk gaan en welke maatregelen je kunt nemen om je bedrijf te beschermen. Maar waar sta je nu? Is je beveiliging op orde, of loop je meer risico dan je denkt?

Gebruik deze checklist om snel te beoordelen hoe veilig jouw organisatie is.

<STAP1>
VEILIG OMGAAN MET INLOGGEGEVENS EN ONLINE IDENTITEIT

- ☐ Gebruikt iedereen binnen het bedrijf tweefactorauthenticatie (2FA) voor e-mail, boekhouding en andere belangrijke systemen?
- ☐ Worden wachtwoorden opgeslagen in een wachtwoordmanager en niet in browsers of Excel-lijstjes?
- ☐ Zijn zakelijke en privé-accounts gescheiden, zodat medewerkers geen werkgerelateerde accounts gebruiken op onbeveiligde privéapparaten?
- ☐ Wordt toegang tot systemen direct ingetrokken zodra een medewerker uit dienst gaat?

<STAP2>
BACK-UPS EN HERSTELBAARHEID

- ☐ Worden er dagelijks automatische back-ups gemaakt van belangrijke bedrijfsgegevens?
- ☐ Is er minimaal één offline back-up die niet verbonden is met het netwerk?
- ☐ Zijn back-ups versleuteld, zodat ze niet toegankelijk zijn voor onbevoegden?
- ☐ Worden back-ups regelmatig getest door bestanden terug te zetten?

<STAP3>
UPDATES EN PATCHBEHEER

- Worden besturingssystemen, software en apparaten automatisch bijgewerkt met de nieuwste beveiligingsupdates?
- Zijn alle verouderde systemen en software vervangen of uitgeschakeld?
- Zijn alle apparaten en accounts binnen het bedrijf in kaart gebracht, zodat er geen onbeschermde systemen rondslingeren?

<STAP4>
E-MAILBEVEILIGING EN REPUTATIEBESCHERMING

- Zijn SPF, DKIM en DMARC ingesteld om misbruik van je bedrijfsdomein te voorkomen?
- Worden inkomende e-mails automatisch gecontroleerd op verdachte bijlagen en links?
- Worden ongewenste e-mails afgevangen of belanden ze in de inbox?
- Zijn medewerkers getraind in het herkennen van phishing, CEO-fraude en factuurfraude?

<STAP5>
GEDRAGSVERANDERING EN BEWUSTZIJN

- Is cybersecurity een vast onderdeel van de hele bedrijfscultuur en niet alleen een IT-onderwerp? Wordt digitale veiligheid zichtbaar (uit)gedragen door de directie?
- Durven medewerkers verdachte situaties te melden zonder angst voor repercussies?
- Worden er periodieke security-oefeningen uitgevoerd?
- Zijn leveranciers en externe partijen ook onderworpen aan beveiligingsrichtlijnen?

<0-9>
VINKJES

Er zijn serieuze risico's.

Cybercriminelen hebben weinig moeite om binnen te komen. Neem direct maatregelen.

<10-14>
VINKJES

Je hebt een solide basis,

maar er zijn zwakke plekken die aandacht nodig hebben. Tijd om actie te ondernemen.

<15-19>
VINKJES

Jouw organisatie is goed beveiligd,

maar blijf waakzaam en houd cybersecurity een vast onderdeel van de bedrijfsvoering.

</TOT SLOT: CYBERSECURITY IS GEEN PROJECT, MAAR EEN MINDSET>

Veel bedrijven zien cybersecurity als een eenmalig project. Even een paar maatregelen nemen, en klaar. Maar zo werkt het niet.

Cyberdreigingen veranderen continu, en bedrijven die niet meebewegen, lopen een steeds groter risico. Daarom is cybersecurity geen checklist die je één keer afvinkt, maar een mindset die je in je organisatie verankert.

<TOT SLOT>

WAT NU?

- Begin klein, maar begin vandaag. Zelfs simpele stappen, zoals het instellen van tweefactorauthenticatie en het verbeteren van wachtwoordbeheer, maken al groot verschil.
- Maak cybersecurity onderdeel van je bedrijfscultuur. Zorg ervoor dat medewerkers begrijpen waarom het belangrijk is en hoe ze kunnen bijdragen.
- Wees voorbereid op incidenten. Weet wat je moet doen als het misgaat.
  Een goed incidentresponseplan kan de schade beperken en je bedrijf snel weer op de rit krijgen.
- Schakel hulp in als dat nodig is. Je hoeft niet alles zelf te doen. Externe experts kunnen helpen bij beveiligingsscans, incidentresponse en het opzetten van effectieve cybersecuritystrategieën. Wacht niet te lang met hulp inschakelen als je de impact niet overziet.

Cybercriminelen zoeken altijd de makkelijkste prooi. Door de juiste basismaatregelen te nemen, zorg je ervoor dat jouw bedrijf niet op hun lijstje staat.

<WIL JE WETEN>

HOE JOUW ORGANISATIE ER NU VOOR STAAT?

Of heb je hulp nodig bij het verbeteren van je cybersecurity? Neem contact met ons op.
Geen verkooppraatjes, geen bangmakerij — gewoon eerlijk advies over wat wél werkt.

</BONUSFABELS!>

<FABELS>
VPN BIEDT GEGARANDEERDE PRIVACY

Er zijn heel veel VPN-aanbieders, denk aan Proton of NordVPN, maar ze leveren niet meer privacy dan de KPN's en Ziggo's van deze wereld. Soms kan VPN handig zijn om op je vakantiebestemming Netflix of F1TV te kunnen kijken, maar extra veiligheid biedt het zeker niet. Hooguit zorgt VPN ervoor dat het netwerk waarmee je verbindt minder van je verkeer kan zien, maar in ruil daarvoor gaat het naar een provider die misschien nog wel minder betrouwbaar is. Zeker als hun dienst gratis is.

<FABELS>
VIA PUBLIEKE WIFI KAN JE ZÓ GEHACKT WORDEN

Je wordt vaak gewaarschuwd om je laptop of smartphone niet aan te melden op publieke wifi-punten, aangezien je data dan door een kwaadwillende onderschept kan worden. Echter, voor zo'n illegale actie moet een hacker ongeveer naast je komen zitten.

De meeste mensen zijn gewoon niet interessant genoeg om het risico te lopen om gesnapt en gearresteerd te worden. Heb jij wél zo'n aantrekkelijk profiel voor een hacker, dan adviseren we je om je smartphone in te leveren en een anonieme Nokia te gaan gebruiken.

<FABELS>
IK HEB OVERAL HETZELFDE WACHTWOORD, WANT IK BEN TOCH NIET INTERESSANT

Over wachtwoorden horen we misschien wel de meeste wilde verhalen. Er zijn maar twee dingen belangrijk: de lengte van het wachtwoord en dat het uniek is. Zet je wachtwoorden in een wachtwoordmanager, of desnoods in een boekje: dat is nog altijd beter dan overal hetzelfde wachtwoord. Veranderen hoeft alleen als er een aanleiding voor is, bijvoorbeeld als de organisatie een datalek heeft gehad of er een indicatie is van een security-incident.

<FABELS>
MULTIFACTORAUTHENTICATIE OF 2FA GEEFT 100% DIGITALE VEILIGHEID

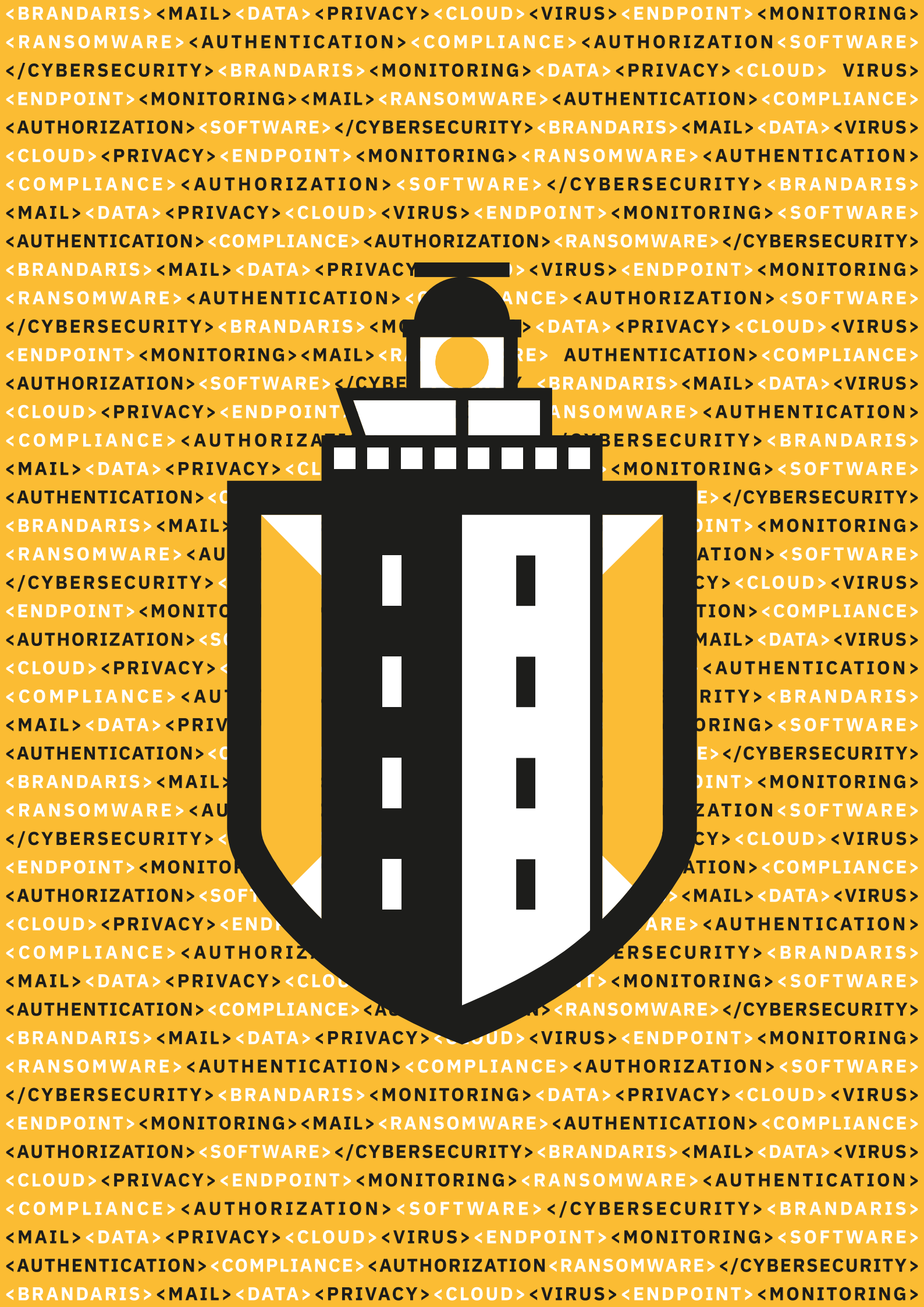
Zeker, 2FA geeft je accounts meer bescherming, maar het kan hacken nooit gegarandeerd voorkomen. Er zijn inmiddels vormen die zogeheten phishing-bestendig zijn (zoals Passkeys, waarbij ook de website wordt gecontroleerd), maar dit brengt wel de nodige extra complexiteit mee. Je moet meer handelingen uitvoeren, dus meer gedoe in ruil voor meer veiligheid. Multifactorauthenticatie heeft dus absoluut toegevoegde waarde, maar het is een fabel dat je hiermee onaantastbaar bent.



<BRANDARIS CYBERSECURITY B.V.>
Kalkovensweg 6b
1815 KZ Alkmaar

+31 (0)72 202 97 95
info@brandaris.it
www.brandaris.it

<KVK> 94696675
<BTW> NL866862833B01
<IBAN> NL58REVO7619561102
<BIC> REVONL22


<BRANDARIS><MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING>
<RANSOMWARE><AUTHENTICATION><COMPLIANCE><AUTHORIZATION<SOFTWARE>
</CYBERSECURITY><BRANDARIS><MONITORING><DATA><PRIVACY><CLOUD> VIRUS>
<ENDPOINT><MONITORING><MAIL><RANSOMWARE><AUTHENTICATION><COMPLIANCE>
<AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS><MAIL><DATA><VIRUS>
<CLOUD><PRIVACY><ENDPOINT><MONITORING><RANSOMWARE><AUTHENTICATION>
<COMPLIANCE><AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS>
<MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING><SOFTWARE>
<AUTHENTICATION><COMPLIANCE><AUTHORIZATION><RANSOMWARE></CYBERSECURITY>
<BRANDARIS><MAIL><DATA><PRIVACY><VIRUS><ENDPOINT><MONITORING>
<RANSOMWARE><AUTHENTICATION><ANCE><AUTHORIZATION><SOFTWARE>
</CYBERSECURITY><BRANDARIS><DATA><PRIVACY><CLOUD><VIRUS>
<ENDPOINT><MONITORING><MAIL><RE> AUTHENTICATION><COMPLIANCE>
<AUTHORIZATION><SOFTWARE><BRANDARIS><MAIL><DATA><VIRUS>
<CLOUD><PRIVACY><ANSOMWARE><AUTHENTICATION>
<COMPLIANCE><BERSECURITY><BRANDARIS>
<MAIL><DATA><PRIVACY><MONITORING><SOFTWARE>
<AUTHENTICATION><E></CYBERSECURITY>
<BRANDARIS><MAIL><INT><MONITORING>
<RANSOMWARE><ATION><SOFTWARE>
</CYBERSECURITY><CY><CLOUD><VIRUS>
<ENDPOINT><MONITO><TION><COMPLIANCE>
<AUTHORIZATION><S><MAIL><DATA><VIRUS>
<CLOUD><PRIVACY><AUTHENTICATION>
<COMPLIANCE><AU><RITY><BRANDARIS>
<MAIL><DATA><PRIV><ORING><SOFTWARE>
<AUTHENTICATION><C><E></CYBERSECURITY>
<BRANDARIS><MAIL><INT><MONITORING>
<RANSOMWARE><AU><ZATION><SOFTWARE>
</CYBERSECURITY><CY><CLOUD><VIRUS>
<ENDPOINT><MONITO><ATION><COMPLIANCE>
<AUTHORIZATION><SOFT><MAIL><DATA><VIRUS>
<CLOUD><PRIVACY><END><ARE><AUTHENTICATION>
<COMPLIANCE><AUTHORIZ><ERSECURITY><BRANDARIS>
<MAIL><DATA><PRIVACY><CLO><T><MONITORING><SOFTWARE>
<AUTHENTICATION><COMPLIANCE><A><RANSOMWARE></CYBERSECURITY>
<BRANDARIS><MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING>
<RANSOMWARE><AUTHENTICATION><COMPLIANCE><AUTHORIZATION><SOFTWARE>
</CYBERSECURITY><BRANDARIS><MONITORING><DATA><PRIVACY><CLOUD><VIRUS>
<ENDPOINT><MONITORING><MAIL><RANSOMWARE><AUTHENTICATION><COMPLIANCE>
<AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS><MAIL><DATA><VIRUS>
<CLOUD><PRIVACY><ENDPOINT><MONITORING><RANSOMWARE><AUTHENTICATION>
<COMPLIANCE><AUTHORIZATION><SOFTWARE></CYBERSECURITY><BRANDARIS>
<MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING><SOFTWARE>
<AUTHENTICATION><COMPLIANCE><AUTHORIZATION<RANSOMWARE></CYBERSECURITY>
<BRANDARIS><MAIL><DATA><PRIVACY><CLOUD><VIRUS><ENDPOINT><MONITORING>