Whitepaper
Cyberveiligheid op de werkvloer

ABN·AMRO

Inhoud

1. Cybercriminelen worden steeds professioneler

De dreiging van cybercriminaliteit neemt snel toe. Cybercriminelen richten zich steeds vaker op MKB-bedrijven, omdat die hun beveiliging niet altijd even goed op orde hebben. Met allerlei soorten aanvallen proberen criminelen data te stelen of gijzelen ze bijvoorbeeld systemen voor losgeld. Zonder de juiste maatregelen staat de digitale deur ongemerkt op een kier, en kunnen cybercriminelen hun gang gaan.

Impact van cybercriminaliteit

Een serieus datalek kost gemiddeld 4 miljoen euro. Dat gaat om zowel directe als indirecte schade, inclusief eventuele imagoschade en andere gevolgen. Jaarlijks krijgen in Nederland zo'n 50.000 MKB-bedrijven te maken met cybercrime. Het is een groeiend risico, dat om een professionele aanpak vraagt.

Cybercriminelen stelen data of proberen systemen plat te leggen. Met ransomware gijzelen ze data en/of systemen, waardoor processen stilvallen en bedrijven niet verder kunnen. Daarnaast neemt het aantal gecompromitteerde systemen door hacks toe.

Criminelen krijgen toegang tot het bedrijfsnetwerk, breken in op het communicatie- en/ of transactieproces en sluizen vervolgens ongemerkt bedragen weg.

Typische aanvallen op MKB-bedrijven

Malware uit e-mails en andere berichten
Cybercriminelen sturen e-mails, sms-berichten en WhatsApp-berichten met links naar malware. Wie op de foute links klikt of gevaarlijke bijlagen opent loopt het risico om ongemerkt schadelijke software te installeren.

Social engineering bij medewerkers
Medewerkers vormen vaak ongemerkt de zwakke schakel in een organisatie. Cybercriminelen richten zich op hen met berichten die niet van echt te onderscheiden zijn. Training in cyber security awareness verkleint de risico's.

Exploitatie van technische kwetsbaarheden
Naleving van de belangrijke normen voor informatiebeveiliging (ISO 27001 en NEN 7510) verkleinen en voorkomen de belangrijkste risico's. Voorkom exploitatie van technische kwetsbaarheden, bijvoorbeeld door achterstallig onderhoud of het te laat installeren van updates.

Problemen met de veiligheid bij leveranciers
Neem leveranciers, klanten en andere partners mee als het gaat om cybersecurity. Voorkom dat een lek of zwakke beveiliging bij hen, leidt tot problemen met data of systemen binnen uw eigen organisatie.

2. Medewerkers zijn favoriete doelwit

Maar liefst 85% van de cyberincidenten ontstaat door social engineering, dus door aanvallen op medewerkers zoals jij. Vooral e-mails vormen een belangrijk risico. In 58% van alle gevallen weten cybercriminelen via e-mail malware te verspreiden of inloggegevens te bemachtigen. Daarnaast is 77% van de cyberaanvallen specifiek gericht op mensen en gaat het in 59% van de gevallen om gerichte diefstal van data. Vooral in de financiële sector vormt dit een groot risico. Bijna 9 op de 10 medewerkers in die sector kwam al eens in aanraking met een vorm van social engineering. Het risico dat ook u hiermee te maken krijgt is groot.

Eenvoudiger te manipuleren dan de technologie

Als u zich als medewerker bewust bent van de veiligheidsrisico's en de noodzaak om veilig met data en systemen om te gaan verbetert u de bescherming. Zonder risicobewustzijn bij medewerkers lopen organisaties onnodig grote risico's. Security awareness staat voor de mate waarin medewerkers bewust zijn van de risico's die zij (en de organisaties waar ze werken) lopen.

De mens blijkt in de meeste gevallen van cybercrime de zwakke schakel. Mensen klikken onwetend op links in phishing emails, delen onbewust informatie met cybercriminelen of zetten op andere manieren ongemerkt de deur op een kier.

Let op!
77% van de cyber-aanvallen zijn specifiek gericht op mensen. Vooral in de financiële sector vormt dit een groot risico.

Vormen van social engineering

Cybercrime gericht op medewerkers noemen we social engineering. Social engineering kent verschillende vormen. Het gaat om fysieke social engineering waarbij kwaadwillenden meekijken (shoulder surfing), afval doorzoeken (dumpster diving) of besmette USB-sticks verspreiden. Daarnaast doen criminelen zich voor als iemand anders of proberen ze u af te leiden. Vooral digitale social engineering vormt een steeds groter risico. Verdiep u daarom bijvoorbeeld in:

Phishing, smishing en spoofing
Herken de pogingen die cybercriminelen doen om gegevens te stelen of toegang te krijgen tot systemen. En herken valse e-mails, sms-berichten en andere berichten.

Business Email Compromise (BEC)
Je ontvangt een e-mail van cybercriminelen, die afkomstig lijkt van een leverancier of klant of zelfs van een collega. De interne e-mail komt eigenlijk van buitenaf, met als doel om toegang te krijgen tot informatie en/of systemen.

Voice solicitation
Je ontvangt telefoontjes van cybercriminelen, die zich voordoen als iemand anders. Ze stellen zich voor als collega's of zelfs een leidinggevende. Spreek met uzelf af om altijd te controleren met wie u heeft gesproken.

Helpdeskfraude
Criminelen doen zich voor als een medewerker van de helpdesk, van de bank, Microsoft of een andere softwareleverancier. Ze vragen u om gegevens te delen, die cybercriminelen daarna gebruiken om data te stelen of systemen binnen te dringen.

Nepfacturen
Je ontvangt valse facturen van cybercriminelen. Ze gebruiken hiervoor gegevens die lijken op die van een leverancier, vaak met een rekeningnummer dat slechts één of een paar karakters afwijkt.

CEO-fraude
Cybercriminelen doen zich voor als de CEO, CFO of een andere executive binnen de organisatie. Ze geven u de opdracht om gegevens te delen of om een bedrag over te boeken, terwijl de werkelijke CEO of CFO van niets weet.

Social media scams
Cybercriminelen gebruiken nep-accounts om connecties aan te gaan met u en uw collega's. Nadat ze een band hebben opgebouwd sturen ze een bijlage of link waarmee ze malware installeren of toegang krijgen tot systemen.

3. Cyberveiligheid verhogen

Bescherm de organisatie samen met uw collega's tegen aanvallen van buitenaf. Uw werkgever gebruikt daarvoor de belangrijke normen voor informatiebeveiliging zoals ISO 27001 en NEN 7510 als uitgangspunt.

Voorkom of beperk samen het risico dat cyber-criminelen kunnen binnendringen. Zorg voor een goede basishygiëne voor cyberveiligheid en train uzelf en uw collega's om alert te zijn en de beveiliging te verbeteren. Houd er rekening mee dat alleen kennis van de risico's niet genoeg is, het gaat ook om uw houding en gedrag om de veiligheid te verbeteren. Denk bijvoorbeeld aan het melden van verdachte e-mails.

Training van medewerkers

Betere beveiliging begint met meer security awareness bij medewerkers. Pas als u zich bewust bent van de risico's kun u u daarnaar gedragen en de veiligheid verbeteren.

Tegelijkertijd betekent meer kennis van cyber-beveiliging en de -risico's niet automatisch veiliger gedrag. Sterker nog, gedragsverandering bij medewerkers is vaak de grootste uitdaging voor bedrijven die hun cyberveiligheid willen verbeteren. Zorg daarom dat u er in de praktijk mee aan de slag gaat.

Phishing tests & Voice solicitation tests

Oefen samen met collega's in de praktijk. Terwijl slechts 13% van de medewerkers gegevens invult na klikken op een phishing e-mail deelt maar liefst 70% een wachtwoord met een onbekende 'collega'.

Werkgevers gebruiken op een vergelijkbare manier voice sollicitation tests. U ontvangt een telefoontje zogenaamd van een collega of leverancier, met een verzoek om data of toegang tot een bepaalde folder. Telefonische verzoeken komen steeds vaker voor, als variant op phishing e-mails die veel mensen na hun training beter herkennen. Met deze trainingen wordt u steeds beter in het herkennen van cybercrime.

Gamification

Gamification maakt gedragsverandering makkelijker en leuker. In spelvorm blijkt 80% van de mensen gemotiveerd om te leren. Gamification verleidt u samen met uw collega's om mee te doen en het verhoogt de engagement die jullie ervaren. In spelvorm lukt het beter om gedragsverandering door te voeren. Door er actief mee te oefenen leert u manieren om risico's te herkennen, daar niet in te trappen en ze op de juiste manier te rapporteren.

Een oefening is bijvoorbeeld een phishing-test:

Uw organisatie (of een extern cyber security trainingsinstituut) verstuurt een test phishing mail over bijvoorbeeld een te ontvangen pakket, een verzoek om een wachtwoord te resetten of een aankondiging van een aanstaande reorganisatie. Na een klik belanden de medewerkers op een pagina die uitlegt dat het om een test gaat en hoe ze de e-mail als phishing hadden kunnen herkennen.

Stimuleer intrinsieke motivatie

Intrinsieke motivatie vraagt om voldoende bewustzijn én een concreet handelingsperspectief. Zorg dat u inziet wat de risico's zijn én leer hoe u moet handelen. Houd andersom rekening met gedragsremmende factoren bij u en bij collega's, zoals:

- Overschatting eigen kennisniveau ('Ik denk dat ik goed op de hoogte ben')
- Onderschatting risiconiveau ('Mij overkomt dat niet')
- Historie eigen inzet ('Ik werk al veilig')

Beveiliging van wachtwoorden en tokens

Verdiep u in de risico's van zwakke wachtwoorden en de kwetsbaarheid door verloren tokens. Train uzelf in het regelmatig wijzigen van hun wachtwoorden en deel tips voor slimmer wachtwoordbeheer. Waarschuw ook voor het hergebruik van wachtwoorden. Gebruik een duidelijk (beveiliging)beleid voor tokens, pasjes en andere fysieke toegangsmaterialen. Denk na over de praktijk waarin u en collega's die gebruiken, om het ze zo makkelijk mogelijk te maken om daarmee om te gaan. Gebruik een wachtwoordmanager, om verschillende wachtwoorden te beheren.

Melden verdachte e-mails en incidenten door medewerkers

Ontwikkel een manier om verdachte e-mails en andere cyberincidenten te melden. Vraag ook collega's om de incidenten intern te melden én meld dat bijvoorbeeld bij de Fraude Helpdesk. Leer hoe u phishing en andere valse berichten herkent. Gebruik een centraal meldpunt, bijvoorbeeld bij de IT-afdeling en borg follow-up acties.

Basishygiëne voor cyberveiligheid

Iedere organisatie zou minimaal de basishygiëne voor cyberveiligheid op orde moeten hebben. Het gaat dan bijvoorbeeld om:

Antivirussoftware en een firewall
Gebruik software die waarschuwt bij virussen, aanvallen van buitenaf en andere dreigingen voor de data, systemen en het netwerk binnen de organisatie.

Tijdige updates en patches ter beveiliging
Achterstallig onderhoud door ontbrekende updates en patches vormen een belangrijk cyberrisico. Cybercriminelen zoeken naar deze zwakke plekken in de beveiliging. Houd alle software dus up-to-date.

(Automatische) back-ups van belangrijke data en systemen
Maak automatisch back-ups van belangrijke data en systemen, om altijd terug te kunnen keren naar de vorige situatie zonder veel verlies aan data. Zorg ervoor dat tenminste een recente back-up offline wordt bewaard.

Actieve monitoring van het netwerk en systemen
Monitor het netwerk en de systemen om een eventuele aanval door cybercriminelen in een zo vroeg mogelijk stadium te herkennen. Kom in actie bij verdachte datastromen naar externe IP-adressen.

Doorlopende training van medewerkers in cybersecurity
Train uzelf in cybersecurity. Vergroot hun kennis over cyber security en ga aan de slag met gedragsverandering om de veiligheid te verbeteren.

Help uzelf en collega's

Help uzelf en collega's door samen doorlopend te trainen, te bedanken en belonen. Beloon goed en veilig gedrag, om ook anderen te stimuleren dat gedrag te vertonen. Klikken op een testmail is geen fout, maar een leermoment. Medewerkers die op een testmail klikken komen uit op een landingspagina die hen leert hoe ze de e-mail als phishing hadden kunnen herkennen. Zo leren ze een wijze les.
Voorkom schaamte door collega's hier niet publiekelijk op aan te spreken. Doe dat liever individueel en laat met tips zien hoe iemand de volgende keer phishing kan herkennen.

Geef feedback op gemelde mails en incidenten

Bedank en beloon anderen die e-mails of andere incidenten melden. Koppel concrete beloningen aan veilig gedrag. Maak collega's trots, bijvoorbeeld door hun melding publiekelijk bekend te maken. Of ga daarop door in de volgende nieuwsbrief, om goed gedrag een podium te bieden. Koppel de opvolging altijd terug aan de medewerker die de melding deed. Laat zien wat er mee gebeurt. Stimuleer op die manier collega's om vaker melding te doen.

Gebruik een report phishing button en wachtwoordmanager

Gebruik een knop om phishing te melden, zoals de Report Phishing Button voor Office 365 van Microsoft. De knop in Microsoft Outlook of andere e-mailsoftware maakt het makkelijker om phishing te melden. Veilig wachtwoordbeheer vraagt om een wachtwoordmanager, plus een sterk hoofdwachtwoord dat regelmatig wijzigt. De wachtwoordmanager maakt sterke wachtwoorden mogelijk, uniek per website, applicatie of tool. Een zeer sterk en regelmatig wijzigend hoofdwachtwoord of nog beter, een wachtzin voorkomt dat cybercriminelen hier toegang toe krijgen. U hoeft dan alleen nog het hoofdwachtwoord of de wachtzin te onthouden.

4. Veilige omgang met informatie en systemen

Zorg dat u en uw collega's leren hoe ze veilig omgaan met informatie en systemen. Vertel ze over de risico's en laat vervolgens precies zien hoe ze het veiliger kunnen doen.

Toegang tot data en systemen

Regel het toegangsbeheer (access control en access management) voor data en systemen. Bedenk wie tot welke gegevens en systemen toegang moet hebben. Beperk toegang voor iedereen die dat niet nodig heeft. Houd bovendien bij wie waar toegang toe heeft. Gebruik oplossingen voor Discretionary Access Control (DAC), Mandatory Access Control (MAC), op rollen gebaseerd toegangsbeheer (RBAC) of op kenmerken gebaseerd toegangsbeheer (ABAC). Gebruik daarnaast altijd tweefactorauthenticatie of multifactorauthenticatie. Dat is beveiliging met een extra controle. U moet uw inlogpoging bevestigen op bijvoorbeeld een smartphone, via een sms-bericht met een code of een authenticatie-app.

Meervoudige authenticatie combineert:

- Iets dat iemand weet (een gebruikersnaam en wachtwoord)
- Iets dat iemand is (biometrische gegevens zoals vingerafdrukken of gezichtsherkenning)
- Iets dat iemand heeft (een sleutelkaart, token en SMS naar een mobiel apparaat)
- Locatie (voor geografische of netwerkbeperkingen)

Opslaan en delen van informatie

Sla bestanden en andere data altijd versleuteld op. Of beter nog, stel standaardencryptie in als u bestanden opslaat. Door dat automatisch in te stellen hoeft u daar niet over na te denken, dus kunt u het ook niet vergeten.

Houd daarnaast rekening met de Algemene Verordening Gegevensbescherming (AVG). Zorg dat bestanden niet langer dan toegestaan blijven opgeslagen, door de beschikbaarheidstermijn in te stellen.

Buiten kantoor

Train uzelf samen met collega's in de risico's van thuiswerken en via openbare WiFi-hotspots. Bepaal bijvoorbeeld welke apparaten u thuis kan en mag gebruiken, stuur aan op sterke, unieke wachtwoorden en deel onderling tips om het thuisnetwerk goed te beveiligen. Gebruik een VPN-verbinding bij openbare WiFi-hotspots. Versleutel daarnaast webapplicaties of gebruik een Remote Desktop Protocol (RDP) met veilige instellingen.

Tip:
werk met leveranciers voor data- en opslagsystemen met de juiste certificeringen voor informatiebeveiliging (ISO 27001)

Gebruik van applicaties, eigen laptops en systemen

Niet zelf software of plugins installeren
Macro's en andere uitvoerende bestanden vormen een groeiend risico voor cybersecurity. Microsoft-software zoals Word en Excel staan macro's toe om scripts te draaien en automatisering mogelijk te maken. Dat vormt een risico, omdat cybercriminelen die scripts kunnen gebruiken om malware op te halen en schade aan te richten.

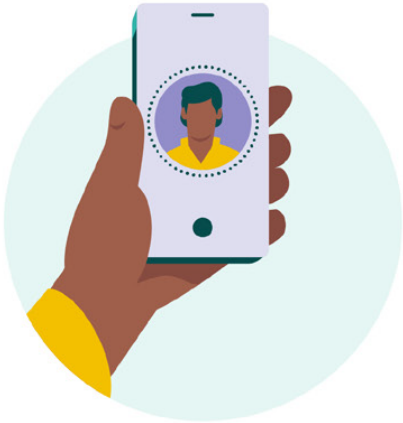
Daarnaast vormt shadow IT een belangrijk risico voor organisaties. Dit is software en hardware die medewerkers gebruiken, zonder dat de IT-afdeling daarvan op de hoogte is. Als u eigen smartphones, tablets, USBsticks of cloudapplicaties zoals Zoom, MOVEit Transfer en TeamViewer gebruikt vormt u daarmee ongemerkt een beveiligingsrisico.

Stel vast welke applicaties en hardware u en uw collega's zakelijk mogen gebruiken. Bespreek dit in goed overleg, om weerstand te voorkomen. Word samen ambassadeur van het beleid, door u te mengen in beslissingen die worden genomen.

Gebruik van cloudservices en SaaS diensten
Cloudservices en SaaS-diensten vormen risico's als de IT-organisatie daar geen toezicht op heeft. Gebruik bijvoorbeeld een Cloud Access Security Broker (CASB) om de cloudtoegang voor gebruikers naar de applicaties te regelen, monitoren en bewaken. Krijg op die manier meer grip op het beveiligingsbeleid.

Social media-profielen en gebruik

Besteed op eenzelfde manier aandacht aan social media. Herken het gevaar van linkjes en bijlagen, leg uit hoe u platformen veilig gebruikt en beperk toegang van apps. Deel geen detailinformatie over uw werkzaamheden op social media. Voer regelmatig een privacycontrole uit of stel de beveiliging en privacy handmatig in. Door hier specifiek tijd voor vrij te maken traint u als medewerker en verhoogt u het bewustzijn van cyberrisico's van sociale media.



5. Doe regelmatig een cyberoefening

Oefen regelmatig met cybersecurity, de risico's en hoe jij en uw collega's daarmee om moeten gaan. Voorkom een schaamtecultuur en haal cyberbeveiliging uit de onbekendheid, door er vaker mee aan de slag te gaan.

Stel specifieke vragen, zoals:

- Hoe gaan we om met een datalek?
- Welke frauderisico's lopen we als bedrijf?
- Wat gebeurt er als systemen niet beschikbaar zijn? Hebben we een plan B?

Werk op basis van die vragen oefeningen uit om hiermee aan de slag te gaan. Ervaar in de praktijk wat er mis kan gaan en wat daarvan de gevolgen zouden zijn. Gebruik gamification en stuur aan op betere beveiliging, meer awareness en minder risico op social engineering. De overheid heeft een Overheidsbreed Cyberprogramma voor bestuurders en overheidsprofessionals. Doe daarmee inspiratie op voor cyberoefeningen en ga daar binnen de eigen organisatie mee aan de slag. Met een Cyber response plan bent u beter voorbereid en kunt u gericht acties ondernemen die de kans op een cyberincident verkleinen en de schade bij een incident beperken. Download hier tips voor het opstellen van een Cyber response plan voor uw organisatie.

Zelf cybermaatregelen treffen of fraude melden?

Ongeveer een op de vijf ondernemers krijgt te maken met cybercriminaliteit. Zo'n cyberincident kan grote gevolgen hebben voor uw bedrijfsvoering, klanten, leveranciers of reputatie. Het treffen van passende maatregelen is daarom essentieel voor elke onderneming.

- Leer meer over de 4-in-1-cyberoplossing Cyber veilig & zeker en verlaag uw cyberrisico's
- Bekijk slimme tools, handige artikelen en cyberwebinars op onze Veilig ondernemen-pagina
- Plan direct een vrijblijvend cybergesprek met een van onze specialisten en ontdek wat u kunt doen
- Meld fraude bij ons, ook als u twijfelt, waarna onze helpdesk u direct verder helpt

Bijlage 1
Nuttige online documentatie

Veilig zaken doen
abnamro.nl/nl/zakelijk/campagnes/cybersecurity/veilig-zakendoen

Digital Trust Center: Incident response plan
digitaltrustcenter.nl/incident-response-plan

Hiscox: Incident response plan
hiscox.nl/documenten/incident-response-plan-CyberClear.pdf

Nationaal Crisisplan Digitaal
ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal

Cynet: Incident response
cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/

Guide for cybersecurity event recovery
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

SANS Institute: An incident handling process for small and medium businesses
sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791

Hulp bij gijzeling door ransomware
nomoreransom.org

Links en bijlagen controleren
virustotal.com

Bijlage 2
Bronvermelding

kvk.nl/advies-en-informatie/veiligzakendoen/cybersecurity/dit-moet-je-weten-over-cybercrime/

emerce.nl/wire/knowbe4onderzoek-n-vier-medewerkers-nederland-wel-eens-slachtoffer-geweest-social-engineering

digitaltrustcenter.nl/informatie-advies/social-engineering

motivaction.nl/actualiteiten/nieuwsberichten/cybersecurity-hoe-zorg-je-voor-bewustwording-en-gedragsverandering

rijksoverheid.nl/onderwerpen/cybercrime-en-cybersecurity/vraag-en-antwoord/phishing

certificering-keuring.nl/8-direct-toe-te-passen-manieren-om-veilig-gedrag-te-belonen

autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/veilig-thuiswerken-tijdens-corona

dezaak.nl/management/personeel/8-tips-voor-als-uw-personeel-social-media-gebruikt/

digitaleoverheid.nl/achtergrondartikelen/schaamtecultuur-rondom-cyberveiligheid-moet-verdwijnen/322901

ABN·AMRO