Whitepaper

Blijf cyberrisico's de baas in het AI-tijdperk

PinkWeb

Share. Care. Anywhere.

PinkWeb
Share. Care. Anywhere.

Whitepaper

Waarom kunstmatige intelligentie een nieuwe trukendoos is voor cybercriminelen

Kunstmatige intelligentie is ‘hot’. De nieuwe technologieën bieden oneindig veel kansen, maar brengen tegelijkertijd nieuwe digitale gevaren met zich mee. Zo wordt het voor cybercriminelen eenvoudiger schadelijke software te ontwikkelen. Met steeds slinksere methoden weten ze medewerkers te misleiden. Het is bijvoorbeeld moeilijker vast te stellen of teksten, foto’s, video’s en spraak wel echt zijn.

Juist voor accountantskantoren betekent het alle hens aan dek. Zij zijn een aantrekkelijk doelwit voor cybercriminelen, omdat accountants veel vertrouwelijke informatie verwerken. Onderschat de vervelende implicaties niet. Je wil boven alles voorkomen dat je kantoor wordt platgelegd en bedrijfsgevoelige gegevens op straat belanden. Bovendien verlangt nieuwe Europese wet- en regelgeving dat accountantsorganisaties hun cybersecuritybeleid op orde hebben.

In deze whitepaper lees je over de groeiende impact van cybercriminaliteit, hoe je je organisatie weerbaarder maakt tegen cybercriminaliteit en vooral ook hoe je je medewerkers bewust maakt van de risico’s. Hoe maak je van hen de sterkste schakel? En hoe zet je AI in om de informatiebeveiliging naar een hoger niveau te tillen?

Inhoud

Hoofdstuk 1
Het veranderende cyberlandschap in 6 trends

Cybercriminelen gaan steeds slimmer te werk. Zeker met de opkomst van nieuwe AI-technologieën breiden zij hun trukendoos verder uit. Wat zijn de laatste ontwikkelingen in cyberland? Gelukkig is er niet alleen maar slecht nieuws. Kunstmatige intelligentie kan ook worden ingezet om organisaties beter te beveiligen.

In november 2022 werd ChatGPT gelanceerd door techbedrijf OpenAI. Sindsdien staan de kranten dagelijks vol over de kansen en risico's van artificial intelligence. ChatGPT kan nieuwe content creëren uit bestaande data. Deze technologie staat ook wel bekend als generatieve AI. Dankzij deze superchatbot kunnen veel werkzaamheden efficiënter worden uitgevoerd, waarvan ook de accountant kan profiteren. Met duidelijke opdrachten - 'prompts' in AI-taal - kun je samenvattingen maken, brieven schrijven of een goed leesbare tekst rond een bepaald thema produceren. De technologie bespaart niet alleen veel tijd, maar is ook laag-drempelig in gebruik.

Overigens is het dringende advies om ChatGPT nooit voor gevoelige informatie te gebruiken. De data worden opgeslagen in de ChatGPT-database. Het kan zomaar gebeuren dat die informatie opduikt in antwoorden van anderen. Alternatieven voor ChatGPT zijn bijvoorbeeld Google Bard en Bing Chat Enterprise van Microsoft. Dit bedrijf claimt dat hun taalrobot de ingevoerde data niet opslaat of deelt. Maar er zijn meer AI-technologieën. Er bestaan al langer programma's die teksten uit bijna elke taal kunnen vertalen. Er zijn steeds betere tools die spraak kunnen omzetten in tekst.

'Kunstmatige intelligentie: een nieuwe trukendoos voor cybercriminelen'

Vrij nieuw zijn programma's die beelden kunnen genereren uit tekstuele beschrijvingen (zoals Dall-E). Met hulp van AI kan tegenwoordig ook steeds makkelijker spraak en videobeeld worden bewerkt tot nieuwe fragmenten. Tenslotte zijn er AI-tools als Github; hiermee hoef je niet meer zelf te kunnen coderen om bepaalde software te schrijven.

Trend 1. Technieken steeds geraffineerder dankzij AI

De opkomst van nieuwe AI-technologieën, zoals ChatGPT, leidt niet alleen tot interessante kansen, maar brengt ook risico's met zich mee. Cybercriminelen maken maar wat graag gebruik van de nieuwe AI-tools. Onlangs waarschuwde de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) voor de grotere cybergevaren van AI-technologieën, zoals onder meer ChatGPT. De AI-technologie biedt criminelen een hulpmiddel om medewerkers steeds geraffineerder in de val te lokken. Phishingmails waren voorheen misschien nog herkenbaar aan spelfouten. Die tijd is voorbij. Dankzij ChatGPT schrijven kwaadwillenden voortaan foutloze mails, ook nog eens in elke taal. De taalrobot haalt daarbij ook informatie van sociale media, waardoor de indruk kan ontstaan dat de afzender een bekende is. Daardoor zijn oplichtingsmails 'meer gepersonaliseerd'. Een teken dat cybercriminelen al massaal gebruik maken van de AI-technologie: in het eerste kwartaal van 2023 nam het aantal phishingmails met 40% toe ten opzichte van vorig jaar.

Het misleiden van medewerkers beperkt zich niet alleen tot tekst. Cybercriminelen combineren verschillende AI-technologieën en bewerken dan wel manipuleren audio- en videobeelden. Zo ontstaan foto's, video's en spraakberichten die nep zijn, maar heel echt lijken. Deepfake-technologieën bestaan weliswaar langer, het aantal laagdrempelige tools neemt toe.

Kortom, dankzij nieuwe AI-technologieën hebben kwaadwillenden een extra stuk gereedschap in handen om toe te slaan. AI breidt de trukendoos uit. De verwachting is dat cybercriminelen in de toekomst nog vaker aan de digitale poorten van bedrijven zullen rammelen. Zowel grote als kleine bedrijven zullen vaker slachtoffer worden van cybercriminaliteit. Het is nog urgenter om alert te blijven en je te wapenen tegen de grotere cyberrisico's.

Trend 2. Ransomware in de lift

Een steeds vaker voorkomend fenomeen is ransomware, ofwel gijzelsoftware. Met deze kwaadaardige software versleutelt een hacker de computers of bestanden van een organisatie. Pas als een bedrijf betaalt, kunnen de ICT-systemen weer gebruikt worden, zo is de belofte van criminelen. Vaak telt een klok op het scherm af om te benadrukken hoeveel tijd je nog hebt om geld over te maken. Het is een lucratief verdienmodel, hackers eisen volgens cybersecurity-experts zo'n 3 tot 5 procent van de jaaromzet van een bedrijf. Het advies is om niet te betalen, zo hou je het verdienmodel immers in stand. Toch kiezen bedrijven vaak eieren voor hun geld omdat het alternatief is dat de organisatie enkele dagen uit de lucht is. Ook dat kost een smak geld.

Ransomware-aanvallers hebben tegenwoordig geen IT-kennis of hackingvaardigheden nodig. Op het Darkweb kunnen ze eenvoudig via een cryptobetaling een ransomware-pakket aanschaffen. Dat kan net als bij een gewone softwareleverancier middels een abonnementsmodel. De hacker kan zelfs terecht bij een klantenservice als hij problemen ondervindt bij zijn aanvalspogingen.

Mede dankzij programma's als ChatGPT is het ontwikkelen van nieuwe malware bovendien makkelijker. Hackers vragen de chatbot eenvoudigweg om een code te genereren met een speciaal doel. Enige ogenblikken later rolt die er ook uit. Zo kunnen technisch minder onderlegde criminelen ook een slinks plan uitvoeren.

Trend 3. Geopolitieke hackers actief

Ook geopolitieke spanningen, zoals de oorlog tussen Rusland en Oekraïne, leiden tot een verhoogd cyberrisico voor bedrijven. Hackersgroepen uit beide landen proberen door middel van cyberaanvallen hun belangen te behartigen. De NCTV constateert dat er in 2022 een opvallende toename was in het aantal cyberaanvallen door hacktivisten. Zij richten zich om symbolische redenen op organisaties, bijvoorbeeld omdat zij opereren in een land dat Oekraïne steunt. In Nederland of andere EU-landen waren er tot dusver nog geen maatschappij-ontwrichtende cyberincidenten. 'Dat is echter geen garantie voor de toekomst,' aldus het NCTV-rapport. Verschillende veiligheidsdiensten, waaronder de NCTV, waarschuwen ook steeds luider voor de toenemende cyberdreiging vanuit China.

Binnen Visma houdt een speciaal team zich 24/7 bezig met digitale dreigingen die wereldwijd op ons af komen. Het Visma Security-team monitort continu welke groeperingen actief zijn, welke acties zij uitvoeren of van plan zijn en welke doelen ze lijken na te streven. Het team adviseert PinkWeb pro-actief.

Trend 4. Multichannel phishing: nòg overtuigender

Tot dusver was het overzichtelijk: phishing gebeurde vooral via de e-mail. Tegenwoordig zetten hackers ook andere kanalen in om medewerkers van organisaties in de val te lokken. Cybercriminelen maken bijvoorbeeld valse websites die sterk lijken op legitieme websites, zo weten ze inloggegevens of persoonlijke informatie van gebruikers te stelen. Maar criminelen gebruiken ook nep-accounts op social media-platformen om vertrouwen te wekken bij potentiële slachtoffers, die vervolgens naar phishing-websites worden geleid om daar gevoelige gegevens af te troggelen. Tenslotte vindt phishing ook vaker plaats via telefoongesprekken. Criminelen doen zich voor als een medewerker van de bank, belastingdienst of verzekeringsmaatschappij om persoonlijke informatie los te krijgen. Ook kruipen ze soms in de huid van een collega of een familielid. Door meerdere communicatiekanalen te combineren, worden phishing-pogingen geavanceerder én overtuigender.

Trend 5. CEO-fraude: vaak urgente actie

Bij deze geavanceerde vorm van cybercriminaliteit doen aanvallers zich voor als de directeur of een andere hooggeplaatste leidinggevende van het bedrijf. Doel is om collega's te misleiden tot het uitvoeren van financiële transacties of het vrijgeven van gevoelige informatie. Criminelen gaan meestal volgens een vast patroon te werk:

- De aanvallers doen eerst grondig onderzoek naar de organisatie en naar de belangrijkste medewerkers, zoals de CEO en andere topmanagers. Ze verzamelen informatie uit openbare bronnen, social media en andere toegankelijke gegevens.
- Met de verzamelde informatie stellen de aanvallers overtuigende e-mails op die lijken te komen van de CEO of een senior manager. Vaak roepen de mails een gevoel van urgentie op. Zo wordt de ontvanger onder druk gezet om snel en zonder al te veel vragen te handelen. Vaak zijn medewerkers van de financiële of boekhoudkundige afdeling het doelwit. Zij worden bijvoorbeeld verzocht geld over te maken naar een bepaalde rekening of gevoelige financiële gegevens te delen.
- Vaak benadrukken de criminelen strikte vertrouwelijkheid. Ze beweren dat het zou gaan om een geheime deal of een overname die (nog) niet bekend mag worden gemaakt aan andere werknemers.

Trend 6. AI verhoogt cybersecurity

Voor zover de gevaren van AI. Er is ook goed nieuws. AI kan goed worden ingezet om de informatiebeveiliging te versterken. AI kan zo gebruikt worden voor het detecteren van dreigingen, het identificeren van zwakke plekken in het netwerk of het beveiligen van systemen tegen aanvallen. AI kan ook helpen om patronen te ontdekken in het netwerkverkeer en verdachte activiteiten duiden. Zo kan er sneller worden gereageerd en kan er actie worden ondernomen voordat er daadwerkelijk schade wordt aangericht.
Een ander voordeel van AI is dat het kan helpen om menselijke fouten te verminderen. Vaak leiden menselijke fouten tot kwetsbaarheden in het netwerk of tot onopgemerkte dreigingen. Het gebruik van AI-technologieën verkleint de kans op fouten en versterkt de beveiliging van het netwerk.

Hoofdstuk 2
Let op de kroonjuwelen; Waarom je als accountantskantoor extra aantrekkelijk bent voor cybercriminelen

Door de almaar toenemende dreiging van cybercriminaliteit zijn robuuste beveiligingsmaatregelen een must voor accountantskantoren. Cybercriminelen azen immers op persoonlijke en bedrijfsgegevens. Maar ook nieuwe Europese wet- en regelgeving verlangt dat accountants de 'kroonjuwelen' van klanten goed beschermen.

Om verschillende redenen vormen accountantskantoren een aantrekkelijk doelwit voor cybercriminelen. Allereerst verwerken accountants vertrouwelijke financiële informatie. Zowel zakelijke als persoonlijke gegevens van klanten zijn buitengewoon waardevol voor cybercriminelen. Denk aan BSN- en rekeningnummers, fiscale en andere data; criminelen kunnen deze gebruiken voor frauduleuze activiteiten zoals identiteitsdiefstal, phishing of financiële fraude.

Daarnaast bedienen accountantskantoren verschillende klanten. Is een hacker eenmaal binnen, dan heeft hij toegang tot een grote hoeveelheid gevoelige informatie. Grotere kantoren lijken misschien interessanter, omdat zij een grotere klantenportefeuille beheren. Maar ook kleinere kantoren zijn geliefd, omdat zij vaak minder geld en energie steken in informatiebeveiliging. Ze gebruiken soms nog verouderde software of hebben een zwak wachtwoordbeleid. Cybercriminelen weten dit en maken daar graag misbruik van.

Verhoogd risico bij gegevens uitwisselen

Zorg dat je de 'kroonjuwelen' van de klant goed beschermt. Mocht je accountantskantoor worden gegijzeld door ransomware, dan wil je niet dat criminelen direct toegang hebben tot de belangrijkste klantgegevens. Het is daarbij veiliger om data in de cloud te bewaren dan op lokale servers, omdat softwareleveranciers dit systeem voortdurend monitoren. Wel is het verstandig om je softwareleverancier kritisch te bevragen hoe zij de informatieveiligheid garanderen.

Realiseer je goed dat de cyberrisico's tijdens verschillende bedrijfsprocessen groter zijn. Dat is bijvoorbeeld op de momenten waarop je documenten of gegevens uitwisselt met de klant. Even per mail een BSN opvragen of een kopie van een paspoort. Het is misschien makkelijk en voor de handliggend, maar het is geen goed idee. Mailen is simpelweg niet veilig. Het uitwisselen van vertrouwelijke gegevens en documenten doe je het meest veilig via een centrale en beveiligde online omgeving. Klanten krijgen met een unieke login toegang tot informatie die alleen voor hen bestemd is. Het kan bovendien gevaarlijk zijn om vertrouwelijke gegevens en documenten gefragmenteerd op verschillende plekken op te slaan. Vorig jaar ondervond een accountants-

kantoor hoe moeilijk het is om data van klanten dan veilig te houden. Weliswaar bewaarde dit kantoor gegevens op een centrale, goed beveiligde plek, maar hadden medewerkers ook allerlei data in persoonlijke mailboxen staan. Stel dat een klant verzoekt om bepaalde data te verwijderen; als kantoor kun je daar misschien niet aan voldoen. Het is, met andere woorden, heel lastig om compliant te zijn als je klantgegevens niet op één centrale plek bewaart.

Soms heeft een kantoor wel als beleid om gegevens op een centrale plek te bewaren, maar gaat het toch mis. Bedenk dat medewerkers in de praktijk vaak voor gemak kiezen boven het naleven van regels en geldende procedures. Dat is riskant. Zorg dat iedereen ervan doordrongen is waarom bepaalde procedures nodig zijn.

Veilig digitaal ondertekenen

Ook tijdens het ondertekenen van stukken bestaat de kans dat het verkeerd gaat. Een accountantskantoor moet er echt zeker van zijn dat de juiste persoon zijn handtekening zet. Een geldige digitale handtekening op een document is essentieel om de rechtsgeldigheid van het document te waarborgen.
Als het accountantskantoor de handtekening niet met zekerheid kan verifiëren, kan dit de deur openen voor vervalsingen en frauduleuze praktijken.

Waarom je een cyberaanval wil voorkomen

Het is verstandig om bij de geschetste risico's stil te staan en beter nog: ze te minimaliseren. Een cyberaanval kan namelijk nare gevolgen hebben. Het kan leiden tot:

Reputatieschade
Als accountant draag je de morele verantwoordelijkheid zorgvuldig met gevoelige financiële gegevens van klanten om te gaan. Als jouw kantoor een datalek veroorzaakt, dupeer je een groot aantal klanten. Hun gegevens zijn immers in handen gekomen van cybercriminelen. Dit kan leiden tot ernstige reputatieschade. Klanten vertrouwen erop dat hun gegevens veilig zijn bij accountantskantoren.

Financiële fraude
Als je als accountantskantoor het slachtoffer wordt van een cyberaanval, kost dat onvermijdelijk veel geld. Cybercriminelen kunnen ransomware installeren en een grote som losgeld vragen. Vaak ligt het bedrag tussen de 3 tot 5 procent van de jaaromzet van het kantoor. Ook als er geen losgeld wordt verlangd, leidt dit vaak tot financiële schade, omdat het bedrijfsnetwerk al snel een paar dagen plat ligt. Heb je geen recente back-ups gemaakt, dan moet er bovendien veel werk opnieuw verzet worden.

Europese wetgeving: NIS 2

Er is nog een belangrijke reden om cybersecurity juist nu extra serieus te nemen. Op Europees niveau is sinds 2023 nieuwe wetgeving van kracht om Europa beter te beschermen tegen de toenemende cybercriminaliteit: NIS 2.
NIS staat voor netwerk- en informatiesystemen. NIS 2 betreft een nieuwe Europese richtlijn. Hiermee wil het Europees parlement de eisen rondom cybermaatregelen aanscherpen. De NIS 2-richtlijn geldt voor bedrijven met meer dan 50 medewerkers of meer dan 10 miljoen euro omzet die essentiële diensten leveren en van belang zijn voor de economie en samenleving. Het gaat om acht sectoren: financiële markten, bankensector, gezondheidssector, transportsector, drinkwatervoorziening, rioolwaterafvoer, energievoorziening en digitale infrastructuur. Daarnaast heeft NIS2 betrekking op organisaties die actief zijn in de digitale dienstverlening, telecommunicatie, chemicaliën, levensmiddelen, post- en koeriersdiensten, overheidsdiensten, platforms voor sociale media, ruimtevaart, afvalbeheer en afvalwaterbeheer.

Het is de bedoeling dat NIS 2 wordt omgezet naar nationale wetgeving. Naar verwachting gebeurt dat voor maart 2024 Tot die tijd is nog niet precies duidelijk aan welke eisen exact moeten voldoen, maar als kantoor kun je je er wel alvast op voorbereiden. Mocht jouw organisatie straks onder de NIS 2 richtlijn vallen, dan zul je een passend beleid voor informatiebeveiliging moeten hebben. Ook kun je alvast nagaan of je klanten onder de nieuwe

Hoofdstuk 3
Zorg dat de basis op orde is - Maak het cybercriminelen niet te makkelijk

Cybercriminaliteit zal alleen maar toenemen. Door enkele basiszaken te regelen, maak je het hackers niet te gemakkelijk. Veel cyberaanvallen zijn te voorkomen als je deze 10 basismaatregelen neemt. Wees ook kritisch naar je softwareleverancier. Vraag hoe de veiligheid is geborgd.

Cybersecurity-checklist: Is bij jouw kantoor de basis op orde?

1. Gebruik passkeys
2. Gebruik veilige wachtwoorden in combinatie met tweestapsverificatie
3. Kies voor een veilige internet-verbinding
4. Voer software-updates uit
5. Gebruik een beveiligde omgeving voor gegevensuitwisseling

6. Gebruik antivirussoftware
7. Maak back-ups en houd deze up to date
8. Beperk de installatiemogelijkheden van software
9. Beperk rollen van medewerkers
10. Kies voor de cloud

1 Gebruik passkeys

Het is de nieuwe trend, niet langer inloggen met wachtwoorden maar met passkeys. Voor de gebruiker is het niet alleen makkelijker - je moet tegenwoordig nogal wat gebruikersnamen en wachtwoorden onthouden en invoeren. Het is momenteel de meest veilige manier om je digitaal te identificeren. Met een passkey log je niet langer in met een gebruikers/wachtwoord. Je krijgt direct toegang tot een website of applicatie via gezichtsherkenning of via vingerafdrukscan op een 'vertrouwd apparaat' zoals je mobiele telefoon of je laptop.

Een passkey biedt snel en automatisch twee lagen van beveiliging. Een gebruiker heeft bijvoorbeeld zijn smartphone nodig én bevestigt met zijn unieke biometrische eigenschappen dat hij het daadwerkelijk is. Steeds meer organisaties ondersteunen passkeys. Ook PinkWeb biedt die mogelijkheid aan, omdat we er sterk van overtuigd zijn dat passkeys de digitale veiligheid vergroten. Waarom? Als er geen gebruikersnamen en wachtwoorden meer nodig zijn, kunnen die gegevens ook niet meer worden gestolen via phishing-methoden.

2 Gebruik veilige wachtwoorden in combinatie met tweestapsverificatie

Cybercriminelen stelen niet alleen wachtwoorden om zo het bedrijfsnetwerk binnen te komen, ze weten wachtwoorden ook makkelijk te 'kraken'. Vooral nu hackers daarbij AI kunnen inzetten, is het achterhalen van een wachtwoord een 'koud kunstje'. Als dieven persoonlijke gegevens hebben gestolen - of achterhalen via social media, zullen ze eindeloos combinaties uitproberen - met je geboortedatum of je naam, of die van je kinderen. Er bestaan AI-programma's die in enkele minuten duizenden variaties voor wachtwoorden proberen. Wachtwoorden met weinig karakters worden sneller gekraakt, omdat er minder variaties zijn. Het advies is: Kies minimaal 12 karakters, gebruik speciale tekens zoals $@% of maak een zin die je makkelijk kunt onthouden. Het beste is om een goede wachtwoordmanager te gebruiken. Deze genereert een sterk wachtwoord, dat automatisch wordt opgeslagen. Zo kun je gemakkelijk voor elke website een veilig wachtwoord instellen.

Als je inlogt met een wachtwoord is het advies een tweefactorauthenticatie (2FA) te gebruiken. Dat verkleint de kans dat hackers toegang krijgen tot het netwerk. Als ze een wachtwoord hebben weten te achterhalen, kunnen ze toch niet zomaar binnendringen. Veel kantoren hebben tweefactorauthenticatie ingesteld, maar medewerkers zetten die vaak uit omdat het teveel 'gedoe' is. Stimuleer collega's om toch 2FA te gebruiken voor accounts op essentiële netwerken. De veiligste manier om een 2FA code te laten genereren is met een Authenticator-app (bijvoorbeeld van Microsoft of Google). Deze code wordt per SMS of per e-mail verstuurd. Nog een voordeel: met een Authenticator-app hoef je geen internetverbinding te hebben.

3 Gebruik een veilige internetverbinding

Leveranciers van apparatuur en software kiezen vaak standaardinstellingen. Het is enorm belangrijk om het standaard wachtwoord van apparaten die op het netwerk beschikbaar zijn direct te veranderen. Doe je dat niet, dan ben je als ondernemer heel kwetsbaar. Het risico bestaat dat apparatuur, software en netwerkverbindingen vanaf internet te benaderen zijn. Zo zet je wel erg makkelijk de digitale deur open voor kwaadwillenden. Zorg ook voor een goede firewall. Dit is vooral belangrijk wanneer je (ook) eigen servers hebt draaien op je netwerk, die toegang van buitenaf hebben.

Daarnaast is het verstandig om geen openbare WiFi-netwerken te gebruiken, bijvoorbeeld als je een keer vanuit een leuke koffiebar werkt. Gebruik dan de 4G- of 5G-verbinding van je telefoon. Kan het echt niet anders, gebruik dan een VPN als je verbinding maakt met een openbaar WiFi netwerk. Een VPN (Virtual Private Network) zorgt voor een versleutelde en beveiligde internetverbinding.

4 Voer software-updates uit

Houd besturingssystemen en programma's altijd up-to-date. Schakel indien mogelijk de optie in om updates automatisch te installeren. Software die veroudert, bevat kwetsbaarheden; cybercriminelen gebruiken die kwetsbaarheden om binnen te komen. Het gaat hierbij niet alleen om je smartphone, computer en printer, maar om alle apparaten (zoals smart devices) die aan het netwerk zijn gekoppeld. Dus denk bijvoorbeeld ook aan smart tv's, lampen, camera's of koffieapparaten. Zorg dat alle devices en software regelmatig en gedurende de volledige gebruiksduur worden bijgewerkt. Doe dat continu, zodra er nieuwe updates worden uitgebracht.

5 Gebruik een beveiligde omgeving voor gegevensuitwisseling

Zorg ervoor dat privacygevoelige informatie veilig gedeeld wordt. Per e-mail vertrouwelijke gegevens versturen, kan echt niet meer. Wijs de klant daar ook op, die ziet het gevaar misschien niet en mailt toch zijn BSN even aan zijn accountant. Ook is het gebruik van een gratis uploaddienst als WeTransfer een slecht idee. Voor het veilig delen van vertrouwelijke informatie gebruik je het liefst één centrale omgeving zoals een klantenportaal.

6 Gebruik antivirussoftware

Een antivirusprogramma scant je apparaten op aanwezigheid van kwaadaardige software (malware). Je leverancier zal er vaak voor zorgen dat de virusscanner regelmatig wordt bijgewerkt zodat je kantoor beschermd is tegen de laatst bekende virussen.

7 Maak back-ups en houd deze up to date

Sla standaard alles op in Microsoft 365 of in de Google Cloud-omgeving. Zo heb je continu realtime back-ups en de mogelijkheid eerdere versies te herstellen. Zo beschik je over de meest recente gegevens als er onverhoopt iets misgaat. Het is verstandig om ook back-ups van je netwerk en systemen te maken. Bewaar deze in de cloud, als een digitale kluis.

8 Beperk de installatiemogelijkheden van software

Het is niet verstandig als medewerkers zelf software kunnen installeren op bedrijfscomputers. Door dit te beperken, kun je voorkomen dat er mogelijk besmette programma's worden geïnstalleerd. Installeer daarnaast alleen apps die noodzakelijk zijn voor jouw bedrijfsvoering. Hoe meer apps je installeert, hoe groter de kans op online bedreigingen.

9 Beperk rollen van medewerkers

Definieer voor elke medewerker tot welke systemen en data hij of zij toegang nodig heeft om zijn werk goed te kunnen doen. Let erop dat toegangsrechten worden aangepast als iemand een nieuwe functie krijgt of het kantoor verlaat. Dit is extra belangrijk als een collega niet vrijwillig afscheid neemt van het kantoor.

Als een accountantskantoor software gebruikt, die kan worden aangesloten op Microsoft Active Directory, is dat een voordeel. Het kantoor kan de toegang tot diverse diensten in één keer intrekken door het centrale account uit te schakelen. Dit principe staat bekend als automatische provisioning, ook de software van PinkWeb biedt deze mogelijkheid.

10 Kies voor de cloud

Veel kantoren maken voor hun boekhoud- en aangifteprogramma's gebruik van eigen servers. Maar dat maakt ze kwetsbaar. Uiteindelijk hebben kleinere kantoren niet de kennis in huis om de veiligheid te waarborgen en is het voor grote kantoren vaak ook geen kernactiviteit. Het is beter om een clouddienst te gebruiken, omdat de leveranciers er alles aan doen om de veiligheid te waarborgen.

Wees kritisch op IT-leveranciers; stel de juiste vragen met deze checklist

Een goed beveiligd netwerk hangt samen met de keuze voor de juiste IT-software-leverancier. Wanneer je overweegt om software af te nemen van een leverancier, is het belangrijk enkele kritische vragen te stellen hoe het bedrijf cyberveiligheid borgt.

Met onderstaande checklist weet je welke vragen je in elk geval moet stellen aan potentiële IT-leveranciers over informatiebeveiliging. Het kan geen kwaad om ook je bestaande software-leveranciers eens kritisch tegen het licht te houden.

Fysieke beveiliging:

- Waar en hoe worden mijn gegevens vastgelegd, opgeslagen en gebruikt?

Gegevensbeveiliging:

- Hoe wordt mijn informatie beschermd? Zowel in 'rust' als bij het uitwisselen?
- Hoe gaat de leverancier om met netwerkuitval?

Beveiliging van toepassingen:

- Hoe gaat de leverancier om met authenticatie, autorisatie en accountbeheer?
- Wat is de benadering van identiteits- en toegangsbeheer (IAM)?
- Bieden jullie een flexibele, schaalbare oplossing?

Continue bewaking:

- Doet de leverancier aan proactieve monitoring en heeft het een actief beveiligingsbeleid?
- Welke procedures zijn er om verdachte online activiteiten te detecteren en te isoleren?

Beveiligingsbeoordelingen:

- Heeft de leverancier een proactief programma van externe beveiligingsaudits?
- Hoe gaat de leverancier om met de voort-durende naleving van regelgeving, zoals GDPR?
- Heeft de leverancier een gepubliceerde beveiligingsverklaring die ik kan lezen?
- Is de leverancier gecertificeerd volgens wereld-wijde standaarden zoals ISO 9001 en ISO 27001 of heeft de leverancier zelfs een ISAE 3402 type II verklaring?
- Heeft de leverancier een Computer Security Incident Response Team (CSIRT) klaarstaan?

Kies je voor de online omgeving van PinkWeb, dan kun je deze checklist met een gerust hart afvinken. PinkWeb is zich bewust van de grote verantwoordelijkheid om een veilige omgeving te creëren. De beveiliging van de gegevens van klanten en gebruikers wordt dan ook uiterst serieus genomen. De ISAE 3402 Type II verklaring en ISO 27001 en ISO 9001 certificeringen zorgen ervoor dat iedereen in de organisatie continu

ISAE 3402
Type II assured

scherp blijft op het gebied van veiligheid. De collega's zijn voortdurend bezig om de kwaliteit van processen te verbeteren en aan te scherpen. Daarbij is het een groot voordeel dat PinkWeb onderdeel is van de internationale software-groep Visma. Het moederbedrijf hanteert strenge veiligheidsnormen, beschikt over het Visma Security Program en heeft het getalen-teerde Visma Cyber Threat Intelligence Team. De forensische hackers in dit team volgen op het Darkweb of er mogelijke dreigingen zijn voor de Visma-bedrijven, waaronder PinkWeb.

Hoofdstuk 4
Let op de kroonjuwelen; Cindy Wubben (CISO Visma Benelux) roept accountants-kantoren op: *'Steek je kop niet in het zand'*

Naast een goede ICT-hygiëne is een sterke digitale veiligheidscultuur op de werkvloer essentieel om cybercriminelen op afstand te houden. "Zorg dat collega's elkaar onderling scherp houden." Dat is de boodschap van Cindy Wubben, Chief Information Security Officer bij Visma Benelux. Als Chief Information Security Officer Benelux is Cindy Wubben sinds 2021 verantwoordelijk voor informatiebeveiliging binnen de Visma Group. Al ruim 15 jaar houdt Wubben zich bezig met security, ze deed ervaring op bij banken en softwareleveranciers. Zo groeide Wubben als het ware mee met de professionalisering van cybersecurity. "Destijds was informatie-beveiliging een IT-issue, tegenwoordig is het een strategisch vraagstuk. Het raakt immers alle processen en medewerkers, de urgentie van informatiebeveiliging is groter dan ooit."

Delen van kennis is essentieel

In de strijd tegen de groeiende cybercriminaliteit haalt Visma alles uit de kast om zo veilig mogelijke software te leveren en persoonsgegevens te beschermen. Centraal daarbij staat het Visma Security Program dat hoge standaarden naleeft binnen de industrie. Alle bedrijven van Visma - in Nederland zijn dat er nu ruim 40 - moeten aan dit programma voldoen. Wubben: "Als onderdeel van het programma moeten er voortdurend controles worden uitgevoerd om het veiligheidsniveau op peil te houden. Daarbij worden de Visma-bedrijven onderling uitgedaagd om dit zo goed én zo snel mogelijk te doen. De scores worden bijgehouden in de Visma Security Index. De best scorende bedrijven verdienen een golden of platinum-label."

'Het niet herkennen van een phishingmail, kan iedereen overkomen'

Cindy Wubben, CISO Visma Benelux

Sinds 2018 is softwareleverancier PinkWeb onderdeel van Visma. Een bedrijf waar Wubben met trots over spreekt. "PinkWeb is in de accountancysector zeer actief om het bewustzijn over cybersecurity te vergroten. Het team maakt podcasts en publiceert blogs en whitepapers over hoe klanten hun weerbaarheid kunnen vergroten. PinkWeb straalt daarmee autoriteit uit."
Ook Wubben geeft regelmatig presentaties over cybersecurity, onder meer op de Visma Connected Experience. "Het delen van best practices is essentieel. Als softwareleverancier beschikken we over waardevolle kennis uit onderzoeken, samenwerkingen - met ethische hackers en politie - en ervaringen uit de praktijk."

Geraffineerd in de val lokken

Het bewustzijn in de accountancysector kan nog wel omhoog, meent Wubben. "Grote accountantskantoren hebben hun informatie-beveiliging wel op orde. Maar kleinere kantoren zijn er minder mee bezig. Ze zijn vooral druk met de dagelijkse business." Ze geeft aan te begrijpen dat cybersecurity voor een klein kantoor lastiger te regelen is. "Hoe pak je het aan als je zelf niet de kennis hebt en ook geen gespecialiseerde IT-mensen in dienst hebt?". Wubben adviseert kleinere organisaties om op zijn minst kennis op te doen over de issues die spelen en vooral niet de kop in het zand steken. "Mij overkomt dat niet", hoort ze vaak. Dat is helaas niet zo. Natuurlijk worden de pijlen vaker op specifieke bedrijven gericht. Maar cybercriminelen proberen overal binnen te komen.

‘Data van klanten zijn een goudmijn voor cybercriminelen’

Cindy Wubben, CISO Visma Benelux

Accountantskantoren zijn extra interessant omdat ze over veel vertrouwelijke informatie beschikken, denk aan financiële data, BSN, persoonlijke gegevens. Voor online criminelen is het een goudmijn. De gestolen data bieden ze te koop aan op het dark web - een verborgen deel op internet waar illegaal wordt gehandeld. Kwaadwillenden kunnen die informatie aan elkaar knopen en leggen steeds rijkere profielen aan. Zo kunnen ze mensen heel geraffineerd in de val lokken. Cybercriminelen stelen niet alleen data, maar eisen soms losgeld of leggen je kantoor plat.

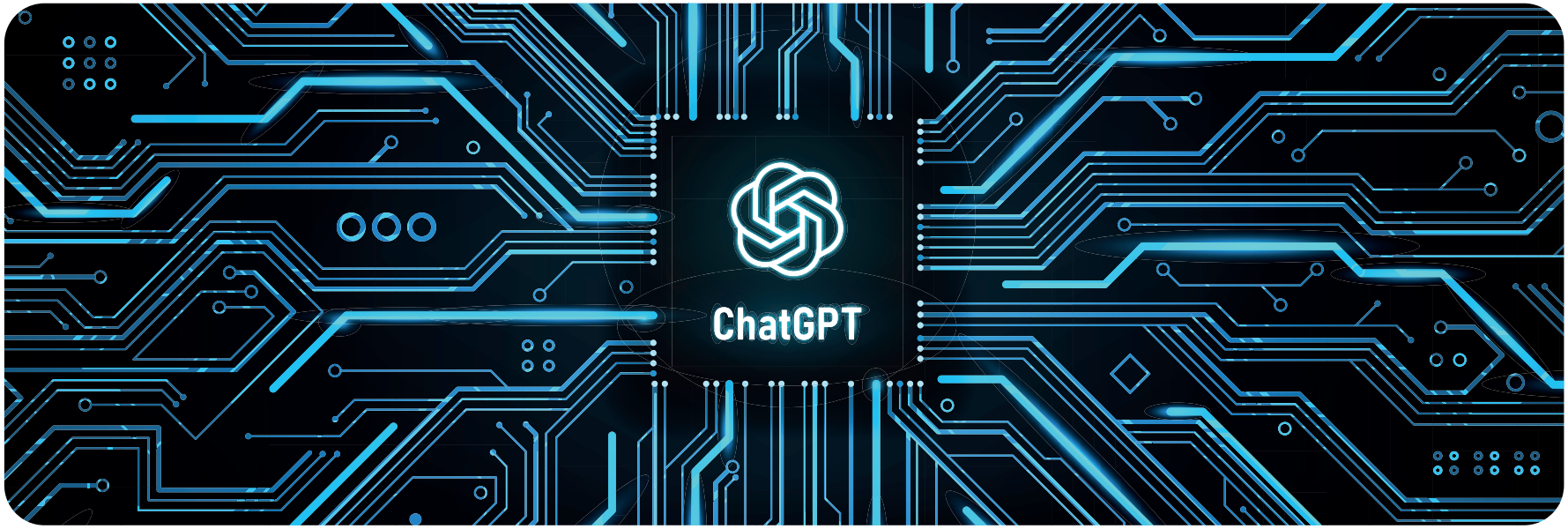
Verschillende verdedigingslinies

Wubben drukt elk kantoor op het hart: “Zorg dat de basis op orde is. Kies voor goede software en voer nieuwe updates direct uit. Cybercriminelen richten zich met geautomatiseerde software op verschillende bedrijven tegelijk en slaan toe als ze gaten in een IT-systeem vinden. Omdat elk softwareprogramma wel foutjes heeft, worden deze door leveranciers voortdurend met nieuwe updates ‘gepatcht’ ofwel gerepareerd. Soms lukt het ook niet”, weet de Visma-CISO Wubben. “Dat betreffen zogenaamde zero-day-aanvallen. Deze cyberaanvallen richten zich op kwetsbaarheden die nog niet zijn opgemerkt, maar enkel bij cybercriminelen bekend zijn.”

Dan nog hoeft er geen reden tot paniek te zijn. “De software van Visma is namelijk gelaagd, ofwel kent diverse verdedigingslinies. Data liggen daardoor niet direct voor het grijpen, maar zijn goed beschermd.”

Niet nerveus

Als CISO is Wubben als geen ander op de hoogte van actuele ontwikkelingen. Ze is niet nerveus over de mogelijk grotere dreiging door nieuwe



technologieën als ChatGPT. “Ik verwacht dat het nieuwe groepen hackers zal aanspreken om hiermee online schade aan te richten. Maar de technieken - zoals het installeren van malware of ransomware - blijven hetzelfde, daarom hoeft de beveiliging vooralsnog niet anders. De gelaagdheid in onze software volstaat. Uiteraard volgen we de ontwikkelingen binnen het security-team kritisch. Overigens is het voor organisaties wel oppassen geblazen omdat de technieken van social engineering nog beter worden dankzij ChatGPT. Doordat beelden en stemmen makkelijker gemanipuleerd kunnen worden, neemt het gevaar op CEO-fraude toe. Zorg ervoor dat je procedures hebt die ervoor zorgen dat een verzoek om geld over te maken altijd extra wordt gecheckt.”

‘In een open leercultuur durven collega’s elkaar aan te spreken op onveilig digitaal gebruik’

Cindy Wubben, CISO Visma Benelux

Creëer een open leercultuur

Wubben benadrukt het belang van een sterke digitale veiligheidscultuur. “Vaak wordt gezegd dat de mens de zwakste schakel is als het gaat om cybersecurity. Maar met de nodige inspanning maak je medewerkers juist tot sterkste schakel.” Hoe je dat voor elkaar krijgt? “Zorg dat een sterke digitale veiligheid breed gedragen wordt. Dat begint bij de directie. Die moet uitstralen dat het thema voortdurend aandacht vraagt. Maar ook op de werkvloer is het goed als alle collega’s zich bewust zijn van de risico’s. En hoe je die beperkt.” Daarbij zou het volgens Wubben goed zijn als er een open leercultuur heerst. “Hier durven collega’s elkaar aan te spreken bij onveilige situaties. Bijvoorbeeld als een collega richting de printer wandelt en een programma open laat staan of wanneer hij een ‘geeltje’ naast zijn scherm met daarop zijn wachtwoord heeft.”

Direct aan de bel trekken

Kantoren kunnen het bewustzijn onder medewerkers vergroten met een awareness-training. Maar die zijn kostbaar, weet Wubben. “Kleinere ondernemers kunnen met een beetje creativiteit zelf een kennisquiz in elkaar zetten. Nodig een cybersecurity-specialist uit voor een presentatie of organiseer een workshop waar collega’s samen veiligheidsproblemen moeten oplossen.”

Sommige bedrijven huren mystery guests in om medewerkers te testen. Soms blijkt dat deze ingehuurde acteurs met een smoes het kantoor kunnen binnenwandelen. Soms lukt het zelfs om toegang tot het bedrijfsnetwerk te krijgen. Wubben is geen groot fan van deze aanpak. “Het is voor medewerkers die de fout ingaan, niet altijd leuk. Die voelen zich voor schut staan. Ik vind het belangrijker dat collega’s fouten mogen maken en elkaar daarop aanspreken.” Dat levert volgens Wubben uiteindelijk meer op.

“In een open leercultuur durven medewerkers immers ook aan de bel te trekken als ze zich realiseren dat ze op een verkeerde link hebben gedrukt.” Het niet herkennen van een phishingmail, kan iedereen overkomen, stelt de CISO van Visma gerust. “Je bent niet altijd even scherp. Bovendien, 80 procent van onze werkzaamheden doen we op de automatische piloot. Het is juist daarom essentieel om veilig digitaal gebruik zoveel mogelijk te stimuleren op de werkvloer. Zo hoort het bij de dagelijkse routine en gaat het niveau van informatie-beveiliging omhoog.”

Hoofdstuk 5 Maak van je medewerkers de sterkste schakel

10 tips om menselijke fouten tot een minimum te beperken

Het gros van alle datalekken en cyberaanvallen is het gevolg van menselijk handelen. Dat is schokkend, maar ook goed nieuws. Door het bewustzijn te vergroten én processen anders in te richten, verlaag je de kans op cybercriminaliteit aanzienlijk.

Uit onderzoek blijkt dat 90 procent van de cybercriminaliteit begint met 'social engineering', ook wel psychologische manipulatie. Cybercriminelen weten internetgebruikers met diverse technieken te verleiden tot het prijsgeven van vertrouwelijke gegevens, toegang te geven tot het systeem of onbewust kwaadaardige malware te installeren. Hackers spelen daarbij in op menselijke eigenschappen als nieuwsgierigheid, vertrouwen, angst en onwetendheid.

Inmiddels is phishing de meest bekende methode. In deze mails, die zogenaamd afkomstig zijn van een instantie of bedrijf, worden gebruikers uitgenodigd om door te klikken op een link of bijlage. Als dat lukt, wordt een virus geïnstalleerd. Maar ook offline lukt het cybercriminelen om toegang tot een netwerk te krijgen. Door bijvoorbeeld bij medewerkers die aan het werk zijn in een gemeenschappelijke ruimte, mee te kijken over de schouders als zij op hun tablet of laptops werken. Ook zo kan een wachtwoord worden buitgemaakt.

Er zijn heel veel verschillende methodes om mensen in de val te lokken.
Terwijl phishing meestal geen gerichte aanval betreft, is spear phishing dat wel. Daarbij wordt een specifieke doelgroep of persoon aangevallen. Vaak de CEO van een organisatie.
Bij phishing bellen hackers op en doen zich bijvoorbeeld voor als IT-medewerker om gegevens te verkrijgen. Bij baiting wordt een valstrik gecreëerd, zoals een USB-stick met malware. Iemand die nieuwsgierig is naar wat er op de stick staat, plaatst deze in zijn USB-aansluiting, waardoor het systeem meteen wordt ontwricht.

Zo vergroot je het bewustzijn bij medewerkers:

1. Organiseer regelmatig een awareness-training

Met een praktische training neemt de bewustwording bij medewerkers toe. Hoe gaan hackers te werk, hoe komen ze binnen? Hoe herken je phishing- en andere technieken? Laat ze vooral ook leren met praktijkvoorbeelden. Herhaal deze trainingen regelmatig.

2. Meten is weten

Om te achterhalen hoe alert jouw medewerkers zijn op cyberrisico's, is het belangrijk om het bewustzijn te meten. Stuur bijvoorbeeld een mail vanuit een onbekend e-mailadres waarin om gevoelige informatie wordt gevraagd. Of stuur een mail met een link naar een 'fake'-internetpagina. Check hoeveel mensen hiermee de fout ingaan en of mensen pro-actief aan de bel trekken dat er iets niet klopt. Door te monitoren, weet je of je misschien het bewustzijn nog wat op moet krikken.

3. Controleer de bron

Een e-mail van je CEO waarin gevraagd wordt om specifieke informatie over individuele medewerkers? Of waarin wordt gevraagd om een groot bedrag over te maken. Bij alle verdachte of afwijkende verzoeken, zouden medewerkers alert moeten zijn. Controleer de opdracht ook eens via een ander kanaal. Kijk ook eens naar de URL, zonder er op te klikken! - vaak is het niet de officiële url. Ook is het e-mailadres vaak net iets anders dan het echte mailadres.

4. Wees op je hoede met deadlines

Social engineering hangt vaak samen met een gevoel van urgentie. Er moet nu betaald worden anders loopt de aanbieding af - aanvallers hopen met dergelijke verzoeken dat hun slachtoffer niet te lang nadenkt over wat er werkelijk aan de hand is. Wees dus altijd op je hoede met deadlines.

5. Vraag altijd om een ID

Een vaak gebruikte social engineering-aanval is door met een hoop dossiers onder de arm naar binnen te lopen. Een behulpzaam type houdt zelfs de deur voor open. Trap er niet in. Vraag altijd om een ID. Dit komt voornamelijk voor bij bedrijven in verzamelpanden.

6. Beperk telefonische informatie

Hetzelfde geldt voor telefonisch contact. Als er wordt gevraagd naar vertrouwelijke informatie, zou het standaardantwoord altijd moeten zijn: 'Namens wie belt u?' Als je het niet vertrouwt, probeer het verzoek altijd via een collega te verifiëren en vertel vriendelijk dat je er op terug zult komen.

7. Wees voorzichtig met gebruik ChatGPT

Misschien gebruiken je medewerkers ChatGPT wel eens om brieven te schrijven of een document samen te vatten. Wijs collega's erop dat het onverstandig is om vertrouwelijke data in te voeren. Dat lijkt vanzelfsprekend. Maar is het misschien niet. Cyberhaven, een Amerikaans cybersecuritybedrijf, onderzocht welke informatie werknemers bij 100.000 bedrijven aan ChatGPT voeren. Hiervan blijkt 11% bedrijfsgevoelig.

8. Zorg voor een what-if scenario

Zorg dat medewerkers op de hoogte zijn als ze per ongeluk op een verkeerde link hebben gedrukt of als blijkt dat dat versleuteld is. Stel een calamiteitenplan op en zorg dat iedereen ervan op de hoogte is. Wie moeten ze bellen in geval van een cyberdreiging. En moeten ze er meteen de internetstekker uit trekken, of juist niet; vaak is het nodig om forensisch onderzoek te doen om te achterhalen of en welke data er zijn gelekt.

9. Voorkom een 'blame'-cultuur

Stel dat een collega zich realiseert dat hij of zij op een link in een phishing-mail heeft geklikt. Het is dan belangrijk dat deze persoon dit direct meldt. Dat zal hij of zij alleen doen als collega's hem of haar niet afbranden. Ook de leidinggevende moet deze persoon niet afrekenen op deze onbedoelde actie. Creëer een cultuur waarin medewerkers alert zijn en continu willen leren om zichzelf te verbeteren.

10. Wijs op risico's bij thuiswerken

Veel medewerkers werken regelmatig een dagje thuis. Voor cybercriminelen is het hybride werken dé kans om ongemerkt toe te slaan. Zeker als medewerkers geen laptop of mobiele telefoon van hun werk hebben maar via hun thuisnetwerk inloggen op het bedrijfsnetwerk. Zorg voor een goede ICT-hygiëne. Geef medewerkers een zakelijke laptop en mobiel als ze thuiswerken. Wijs op de do's & don'ts. Dat het bijvoorbeeld geen goed idee is om minder veilige apps (Facebook of Instagram) of programma's te downloaden op zakelijke apparatuur.

Hoofdstuk 6
Verbeter je informatiebeveiliging met hulp van AI

Omdat veel cyberincidenten het gevolg zijn van menselijke fouten, kun je de informatiebeveiliging flink opschroeven wanneer je handmatige taken zoveel mogelijk automatiseert. Het inzetten van kunstmatige intelligentie en machine learning levert hierbij het meest op.

IVooral bij werkzaamheden die repetitief of tijdrovend zijn, kunnen er wel eens foutjes insluipen. Mensen zijn niet altijd even scherp, ze zijn misschien moe of worden door iets of iemand afgeleid. Het kan dan zomaar gebeuren dat een collega een document deelt met de verkeerde persoon of gegevens onjuist overtikt. Kunstmatige intelligentie kan deze saaie en monotone taken zoals gegevensinvoer of documentverwerking overnemen en daarmee de kans op fouten verminderen. AI werkt immers met constante precisie en efficiëntie. En dat niet alleen. Dankzij machine learning worden computers steeds slimmer. Ze kunnen leren van eerdere ervaringen en zichzelf verbeteren. Dit betekent dat ze beter worden in het vermijden van fouten naarmate ze meer gegevens verwerken.

Steeds slimmer

Het is zowel om veiligheids- als om efficiencyredenen dat PinkWeb er voortdurend naar streeft om zoveel mogelijk handmatige taken te elimineren. Een van de meest recente innovaties is de Signing Hub voor Sharepoint. Dit is een oplossing voor digitaal ondertekenen die gebruikmaakt van AI en machine learning-technologie. De tool bepaalt en herkent zelf het documenttype, voor welke klant het document is bestemd en over welke periode het gaat. Accountants hoeven dus niet meer zelf al deze gegevens handmatig in te vullen. Feitelijk hoef je alleen maar aan te vinken dat je een document wil laten ondertekenen.

Het gebruik van artificial intelligence (AI) vermindert menselijke fouten aanzienlijk

Daar komt nog iets bij: Hoe meer documenten worden aangeboden, hoe slimmer het systeem wordt. Zo kan het systeem met steeds meer zekerheid zeggen om wat voor documenttype het gaat en wat de start- en einddatum van het document is.
Medewerkers besparen met Signing Hub niet alleen veel tijd, ze zullen zo ook minder fouten maken. Het werken met de tool is daarmee sneller en veiliger.

Blijven broeden

PinkWeb zal in de toekomst blijven broeden op slimme manieren waarop mee automatisering kan bijdragen aan het vergroten van de informatieveiligheid én efficiency op kantoren. De missie van PinkWeb is namelijk dat bedrijven niet hoeven te kiezen tussen veiligheid, gemak en efficiëntie. Deze drie pijlers gaan wat ons betreft samen.
We hebben nog veel plannen die we in de toekomst zullen uitrollen om de accountant nòg beter en veiliger te ondersteunen bij zijn werkzaamheden. Zo zijn accountants én klanten ervan verzekerd dat zij hun informatie en documenten onderling veilig kunnen uitwisselen.