unica
ict solutions

&

Microsoft

Whitepaper

De security uitdagingen van 2024

Wij zijn er, altijd.

De feestdagen in december kenmerken traditiegetrouw de overgang naar het nieuwe jaar; het is een moment om even terug te kijken, maar vooral ook vooruit te kijken. Op het vlak van IT-ontwikkelingen en bijbehorende security-uitdagingen heeft 2023 zich zeker als een interessant jaar bewezen en is daarmee ook een opmaat richting 2024. In deze whitepaper kijkt onze specialist op het gebied van security en networking, Hendry Scholing, dan ook graag met je vooruit wat 2024 aan uitdagingen gaat geven en stipt aan waar het niet onverstandig is voor deze ontwikkelingen aandacht te hebben.

Hoe herken je de cybercrimineel anno 2024?

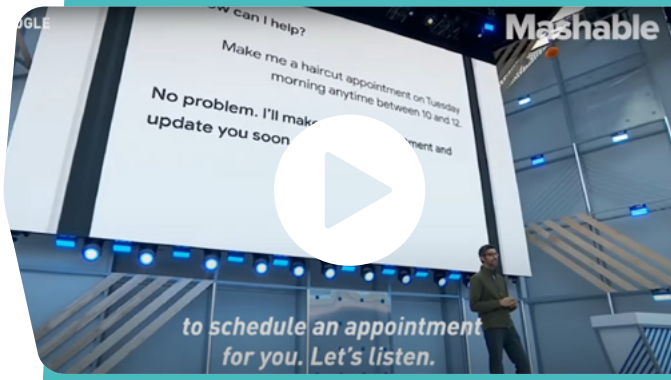
2023 was hét jaar van Artificial Intelligence (AI). De technologiepartners vochten elkaar de tent uit, om vooral maar te laten weten dat hun product nu slim is geworden door de inzet van AI. ChatGPT domineerde het achtuurjournaal, waarbij vooral de keerzijde van kunstmatige intelligentie werd benoemd. Docenten die zich nu moeten verdiepen in de authenticiteit van ingeleverde werkstukken en mogelijke schending van auteursrechten, maar ook de volledige, in luttele seconden gegenereerde, sinterklaasgedichten; het zijn maar enkele van de uitwerkingen die ons bezighielden. AI maakt ons leven een stuk makkelijker, maar we zullen ook om moeten leren gaan met de keerzijde ervan.

Bij Samsung was er het afgelopen jaar een programmeur die via ChatGPT een stuk broncode wilde laten verifiëren. Gevolg; er ontstond direct een datalek. De broncode werd namelijk opgenomen in de openbare informatie van de ChatGPT-omgeving. Niet een handige zet voor het intellectueel eigendom dat op deze broncode rust.

Voor 2024 is het sterke vermoeden dat de inzet van AI ook door de cybercrimineel niet geschuwd zal worden. Een aantal voorbeelden hebben zich de afgelopen jaren al geopenbaard. In 2023 werd een man veroordeeld voor het verspreiden van een stuk porno met in de hoofdrol een deepfake versie van presentatrice Welmoed Sytsma. Met deepfake technologie is het mogelijk om bijvoorbeeld video's en foto's te genereren die echt lijken maar het niet zijn. Hiermee wordt het mogelijk om bijvoorbeeld een filmpje te maken waarin, veelal bekende, personen andere uitspraken doen over gevoelige onderwerpen. Dit kan misschien grappig lijken, maar in sommige gevallen grote gevolgen hebben. Bekijk hier bijvoorbeeld de lijsttrekkers tracks 2023 die tijdens de verkiezingen actueel waren. In dit geval onschuldig, bij sommige politici zie je ook echt duidelijk dat er iets niet klopt, maar sommige politici lijken net echt.

Lijsttrekkers Tracks 2023 - 'Zin in de verkiezingen man!' | Fake It or Leave It | Deepfakes
https://youtu.be/cVrKKob84yM?si=zRCWnU4NPcmAJ9x3

Hoe meer video's en foto's publiekelijk van iemand beschikbaar zijn, hoe realistischer het resultaat zal zijn. Als tegenhanger van video en foto kun je ook denken aan spraaktechnologie. De techniek bestaat inmiddels om stemmen dusdanig te vervormen dat personen denken deze persoon daadwerkelijk te spreken. Dit kan zomaar resulteren in een actie waardoor een secretaresse denkt haar directeur aan de lijn te hebben en er zonder verdere argwaan een opdracht door zal uitvoeren (denk aan het overboeken van geld). Hiermee is de 'next step' in de al bekende CEO-fraude bereikt. Heb je bij het lezen van dit bericht het idee dat dit zo'n vaart nog niet zal lopen? Kijk dan zeker even het filmpje over Google Duplex (deze is inmiddels alweer 5 jaar oud). Het laat je zien dat de Google AI Assistant zelfstandig telefoontjes kan plegen.



Google's AI Assistant Can Now Make Real Phone Calls | Mashable Deals
https://www.youtube.com/watch?v=JvbHu_bVa_g

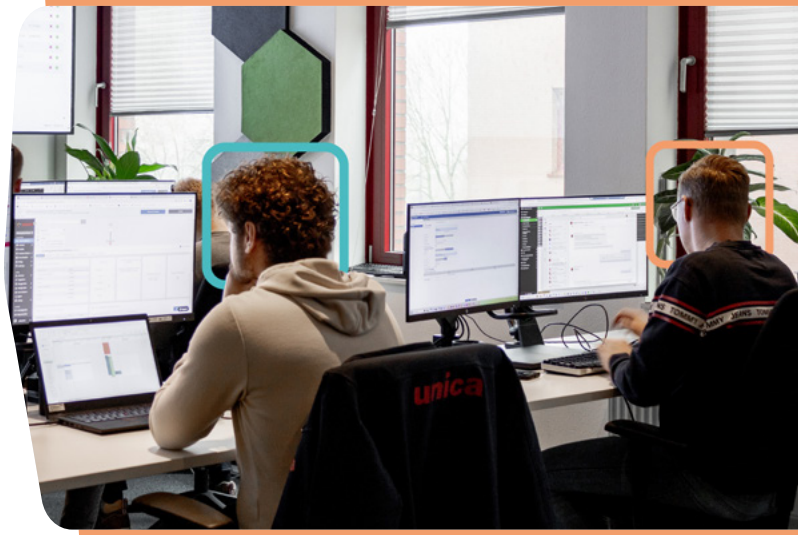
Wil je dit voorkomen? Maak afspraken door bijvoorbeeld een codewoord in je 1 op 1 communicatie te gebruiken als een 2 factor bevestiging. Een buitenstaander zal dit woord niet kennen en daarmee controleer je dus direct de echtheid van de persoon die je wel hoort, maar niet ziet.

Malware, het gaat verder dan je denkt

In 2023 waren ook de nodige ransomwarezaken in het nieuws. Zo was er een prominente plek voor LockBit. LockBit is als oplossing een zogenoemde Ransomware-As-A-Service (RaaS) en wordt gebruikt om geld bij organisaties af te persen. Dat gebeurt door bedrijfsdata te verzamelen en deze vervolgens dreigen publiekelijk te maken. Zoals ieder As-A-Service concept betaamd, wordt deze ransomware-oplossing volledig als dienst aangeboden aan de afperser en wordt de buit gedeeld tussen de afperser en de ontwikkelaars achter LockBit. Ondanks dat LockBit al medio 2019 voor het eerst is gedetecteerd, heeft de oplossing ook de nodige upgrades gehad waardoor ook nu nog steeds diverse organisaties getroffen worden. Zo kwam er in april 2023 het bericht naar buiten dat de KNVB getroffen was. Er werd meer dan een miljoen euro aan losgeld geëist en bij het uitblijven van betaling werd er gedreigd met het openbaar maken van de persoonlijke gegevens van de sterspelers van Team Oranje. Denk aan vermoedelijke kopieën van paspoorten maar ook de inhoudelijk afgesloten contracten.

Later dat jaar verdween de naam van de KNVB van de LockBit-website, wat erop heeft geduid dat de KNVB een som aan losgeld heeft betaald. Dit heeft de KNVB ook bevestigd via haar eigen website. Ook hier ontstond de discussie of het betalen van criminelen wel of niet zwaarder weegt dan de verspreiding van persoonsgegevens. Criminele activiteiten worden tenslotte in stand gehouden door het betalen van losgeld en daarmee wordt de crimineel beloond. Dat de criminelen achter LockBit een soort code van eer hebben bleek trouwens ook in 2023: begin januari stelden ze een stuk software beschikbaar aan een Canadees kinderziekenhuis. LockBit verplicht haar afnemers om dit soort instellingen niet aan te vallen, iets wat helaas toch werd gedaan. De besmetting kon ongedaan gemaakt worden met het beschikbaar stellen van de decryptiesoftware en de afnemer van LockBit was klant af. Dit klinkt eervol, maar het is niet bekend hoeveel schade het ziekenhuis daadwerkelijk heeft geleden door de impact van deze besmetting.

2024 zal wederom een jaar worden waarin de cybercrimineel op steeds geraffineerdere wijze toegang verkrijgt tot de gevoelige data van organisaties. De meeste besmettingen starten nog steeds door het klikken van een link in een e-mail. Berichten krijgen een steeds hogere kwaliteit, waardoor het voor de gebruiker steeds lastiger wordt om een authentiek bericht te onderscheiden van een nep/vervalst bericht. Het is, mede door de ontwikkelingen van bijvoorbeeld AI, belangrijker dan ooit om de medewerker als menselijke firewall te gebruiken. Medewerkers moeten continu getraind worden om de alsmaar nieuwe werkwijzen van de cybercrimineel te blijven herkennen. Een simpele test die meestal één keer per jaar wordt uitgevoerd om een accountant gelukkig te maken is niet langer van deze tijd. Door inzet van goede detectie en response kan veel ellende bespaard worden, het gebruiken van een goede technische Managed of Extended Detection & Response alleen is niet meer afdoende. Juist de combinatie van goed getrainde medewerkers en de inzet van gespecialiseerde securityspecialisten en -diensten is wat 2024 een stukje veiliger zal houden.



Digitale transformatie

Een ander veel voorkomend thema in 2023 was net als voorgaande jaren de digitale transformatie van organisaties. Steeds meer data wordt versnipperd opgeslagen binnen zowel publieke als private cloudoplossingen. Daarbij wordt de data steeds meer decentraal gegenereerd en dient daarmee ook toegankelijk te zijn. Covid heeft vele organisaties gedwongen een vorm van thuiswerken te introduceren en/of uit te breiden. Het bijbehorende informatiebeveiligingsbeleid als ook noodzakelijke technologie werd hierbij uit het oog verloren.

Door de steeds verdergaande digitalisering en opslag van data is het zaak hier nu over na te gaan denken. Dit niet alleen om de data te beschermen tegen bijvoorbeeld lekken, maar ook om een organisatie voor te bereiden op de komst van AI. Zoals al eerder beschreven kan AI bijdragen aan het makkelijker maken van diverse taken, maar kent het ook de nodige keerzijden. AI is zo slim als de data die het wordt aangeboden. Dataclassificatie is dan ook een thema waar organisaties in 2024 nog meer aandacht aan moeten geven. Het kan tenslotte niet zo zijn dat bijvoorbeeld de persoonlijke gegevens uit een HR-systeem per ongeluk bekend worden gemaakt in een door AI aangedreven zoekmachine.

Naast classificatie zul je ook moeten nadenken over de specifieke toegang tot data. Denk bijvoorbeeld aan een Zero Trust architectuur, waarbij alles en iedereen in eerste instantie de status ‘niet vertrouwd’ krijgt en slechts minimale toegang tot bepaalde databronnen krijgt. Heb je bij specifieke data niets te zoeken dan heb je hier standaard ook geen enkel recht op. Dit geldt niet langer alleen maar voor een IT-infrastructuur, maar ook voor een OT-infrastructuur (Operational Technology). Veelal is een OT-infrastructuur, mede vanwege de leeftijd van technologie, extra gevoelig voor een mogelijk cyberaanval.

Daarop aansluitend zal ook bijvoorbeeld netwerktoegang gereguleerd worden door personen alleen via een centraal punt in het netwerk toegang te verschaffen tot data. Dit zal niet langer het netwerk van het kantoor zijn, maar wordt veelal via Cloud-oplossingen geboden waarbij ook direct centraal het beveiligingsbeleid wordt toegepast. Je kunt hierbij denken aan concepten zoals SASE (de Secure Access Service Edge), waarmee gebruikers een consistente ervaring bij het dagelijkse werken krijgen: het maakt veelal niet meer uit waar iemand werkzaam is. Het securitybeleid wordt centraal afgedwongen en daarmee wordt een gelijke ervaring voor de gebruiker gerealiseerd. Het is dan ook een advies om een plekje op de kalender voor 2024 te reserveren om naar SASE-oplossingen te informeren en te onderzoeken hoe deze er voor jouw organisatie aan gaan bijdragen een zo’n optimaal mogelijk beveiligingsplan op te stellen. Onthoudt hierbij wel dat security geen technische oplossing is, maar een proces wat continu bijgestuurd moet worden. Dit kan vrijwillig of bijvoorbeeld door regelgeving worden gestuurd.

De NIS2

In oktober 2024 zal de NIS2 (Network and Information Security directive) van kracht zijn. Op dat moment zijn Europese regels vertaald in specifieke Nederlandse wetgeving. NIS2 is de opvolger van de wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Onder de NIS2-richtlijnen vallen diverse sectoren, die zijn aangemerkt als kritisch onderdeel van onze samenleving. Het aantal sectoren dat het betreft is flink uitgebreid, waarmee de kans groot is dat ook jouw organisatie (direct of indirect) te maken gaat krijgen met deze nieuwe richtlijnen. Reden voor de NIS2-richtlijn is vooral om diverse risico's en bijbehorende impact op het vlak van bijvoorbeeld cybersecurity te verkleinen.

Bedrijven die vallen onder de NIS2 worden verplicht om zich conformeren aan de NIS2-richtlijn, die zich grofweg op Zorgplicht, Meldplicht en Toezicht richt.

Je kunt denken aan het op orde hebben van een goede detectie en response van mogelijke cyberincidenten, maar ook het snel daarop kunnen acteren door een melding te maken bij de toezichthouder. Daarnaast worden bestuurders verplicht gesteld om zich te laten informeren op het gebied van cyberrisico's. Het is daarmee een thema dat op elke agenda van bestuurders moet komen te staan en waarover verantwoording moet worden afgelegd. Voldoe je niet aan de regelgeving dan kunnen er door de toezichthouder hoge boetes worden opgelegd. De NIS2 dwingt organisaties en haar bestuurders daarmee om zich nu meer dan ooit te wapenen tegen cybercriminaliteit. NIS2 zal in 2024 een veelbesproken thema zijn in de boardroom.

Hoef je als organisatie niet te voldoen aan de NIS2-richtlijn? Ook dan is het verstandig om je erin te verdiepen. Jouw organisatie wordt wellicht niet als essentieel gezien volgens de nieuwe richtlijn, maar eventuele gevolgen van een cyberincident kunnen verregaande, tot faillissementen aan toe, gevolgen hebben. Met de grote nasleep van cyberincidenten wil niemand bezig zijn.

Conclusie

2024 zal wederom een bewogen jaar worden op het vlak van cybersecurity, en vooral het jezelf wapenen tegen cybercriminelen. De poging tot het stelen van iemands digitale identiteit is niet voor niets op dit moment het meest geziene securityincident binnen het Security Operating Center van Unica ICT Solutions. Hierbij wordt nog veelal gebruik gemaakt van phishing e-mails. Eenmaal toegang blijken cybercriminelen maanden buiten het beeld van beheerders te kunnen blijven voordat ze gedetecteerd worden. Door inzet van goede technologische oplossingen kan deze tijd sterk verminderd worden en is een investering op dit soort technologie een zeer verstandige keuze. Daarbij is het goed om te beseffen dat niet alleen grote organisaties een potentieel doelwit zijn. Juist ook de kleinere organisaties worden getroffen, omdat er vaak minder budget beschikbaar is voor security. Start dus het nieuwe jaar goed door na te denken over je beveiligingsstrategie en onderneem actie op de plekken waar dit relatief eenvoudig kan. Start, als je dit nog niet gedaan hebt, je securityreis vandaag nog. Het is namelijk niet de vraag of je getroffen kunt worden, maar vooral wanneer. Op dit laatste heb je zelf invloed door de juiste keuzes te maken. Het zal je vast niet verbazen dat de diverse security collega's, voor je klaarstaan om je van een gezonde dosis advies te voorzien. Wellicht is een goede start om eens een security assessment binnen je organisatie uit te laten voeren om daarmee een inzicht te krijgen welke onderdelen direct kunnen bijdragen aan een stukje optimalisatie en waar mogelijk een plan voor moet worden opgesteld. Dit is trouwens niet alleen van toepassing op organisaties die net starten met de optimalisatie van het securitybeleid, maar ook zeker van belang voor organisaties die al langer bezig zijn. Zoals al gesteld is security geen middel, maar een reis die je zult moeten gaan maken. Onderweg zul je daarin keuzes gaan maken.

Heb je vragen of wil je meer informatie?

Hendry wil je graag verder helpen

Hendry is al jarenlang één van de specialisten bij Unica ICT Solutions als het gaat om Networking en Security. Met zijn enthousiasme en kennis geeft hij, vanuit zijn rol als Business Manager Digital Security & Networking, dagelijks advies aan de meest uiteenlopende organisaties, groot of klein. Hij deelt zijn jarenlange deskundigheid graag met zijn collega's en onze klanten en ondersteunt als adviseur ook bij het realiseren, onderhouden en beveiligen van netwerkinfrastructuren. Maar ook alles wat er bij een goede security van een organisatie komt kijken. Nu de infrastructuren het fundament worden voor elke organisatie waarop diensten zoals Microsoft Office365 worden geconsumeerd en ook slimme technologie wordt gekoppeld, is de beschikbaarheid maar ook beveiliging van deze infrastructuren van cruciaal belang. Gebruikers verwachten altijd en overal connectiviteit te hebben, zodat bedrijfsprocessen zo optimaal en veilig gefaciliteerd kunnen worden. Als Solution Specialist op het vlak van security en networking geeft hij een nuchter advies om de optimale, beveiligde en beheersbare infrastructuur voor onze klanten te kunnen realiseren.

Hendry

Business Manager Digital Security & Networking

hscholing@unica.nl
06-54651672

Neem contact op

unica
ict solutions

&

Microsoft

Unica ICT Solutions

ictinfo@unica.nl

unica.nl/ict-solutions

Wij zijn er, altijd.