VAN OERS
it advies

LAATSTE TRENDS EN ONTWIKKELINGEN IN IT EN HOE U GOED BEVEILIGD BLIJFT

Nieuwe IT-ontwikkelingen brengen veel voordelen met zich mee maar kunnen ook de kans op een cybersecurity incident vergroten. Het is daarom van belang dat u op de hoogte blijft van deze nieuwe ontwikkelingen en trends. In deze whitepaper nemen we u mee in de laatste ontwikkelingen op het gebied van IT en cybersecurity en bieden we u handvaten om uw basisbeveiliging up-to-date te houden.

Trends en ontwikkelingen

- Cybercriminelen gebruiken geavanceerde technologieën, en daarom is het nodig om ook geavanceerde technologieën in te zetten voor bedreigingsdetectie en -preventie. AI en machine learning worden steeds meer gebruikt voor realtime analyse van grote hoeveelheden gegevens om bedreigingen te identificeren.
- Met de verschuiving naar de cloud is cloudbeveiliging van vitaal belang. Cloudbeveiligingsmaatregelen, zoals toegangscontrole, encryptie en beveiligingsbewaking voor uw cloud-infrastructuur worden daarmee de standaard.
- Het zogenaamde 'Internet of Things' (IoT) brengt nieuwe beveiligingsuitdagingen met zich mee vanwege de groeiende hoeveelheid verbonden apparaten en is een robuuste beveiliging van IoT-apparaten en netwerken noodzakelijk.
- Ransomware-aanvallen zijn geëvolueerd naar dubbele dreigingen, waarbij aanvallers niet alleen gegevens versleutelen maar ook dreigen met openbaarmaking.
- Aanvallers richten zich vaak op zwakke punten in de toeleveringsketen. Dit betekent dat niet alleen de eigen organisatie maatregelen moet treffen maar ook uw leveranciers. Het is van belang dat u als klant hier zicht op hebt. Assuranceverklaringen zoals een ISAE3402 of SOC2 zijn om die reden waardevol om zicht te krijgen op de maatregelen van uw leverancier.
- Met de opkomst van quantum computing wordt traditionele encryptie kwetsbaarder en dient het gebruik van post-quantum encryptieprotocollen te worden overwogen.

Tips & tricks

Omdat cybersecurity een doorlopend proces is, is het cruciaal om uw strategieën aan te passen en te evolueren om nieuwe en opkomende dreigingen aan te pakken. Houdt daarnaast uw basis op orde en zorg dat uw medewerkers goed opgeleid zijn over de beste beveiligingspraktijken, inclusief hoe ze beveiligingsdreigingen kunnen herkennen en erop kunnen reageren.

Onderstaande tips & tricks kunnen u daarbij helpen.

Werkplek

- Vergrendel altijd uw scherm bij het verlaten van uw werkplek.
- Laat geen gevoelige (klant)gegevens onbeheerd slingeren.
- Een wachtwoord bewaart u nooit op uw werkplek.
- Scherm uw webcam af, bijvoorbeeld met een schuifje.

Flexibel werken

- Beveilig uw wifinetwerk met een sterk wachtwoord en versleuteling.
- Werk regelmatig de firmware van uw router bij.
- Gebruik een Virtueel Particulier Netwerk (VPN) voor extra beveiliging bij het verbinden met openbare wifi.
- Zorg voor een toegangscode of een wachtwoord op uw laptop en telefoon.
- Implementeer beveiligingsmaatregelen voor mobiele apparaten, inclusief de mogelijkheid om op afstand te wissen in geval van verlies of diefstal.

VAN OERS
it advies

Websites

- Laat nooit uw gegevens achter bij websites zonder een slotje voor de URL (HTTPS-verbinding).
- Klik nooit op vreemde pop-ups.
- Bezoek geen illegale websites.
- Bij een beveiligingswaarschuwing van uw webbrowser: sluit de website meteen.

Uw email

- Een vreemde bijlage of vreemde link? Klik hier nooit op.
- Stuur geen reactie op een vreemde mail.
- Weet hoe u een phishing mail kunt herkennen.
- Rapporteer een phishing mail altijd.

Wachtwoorden

- Maak complexe wachtwoorden, minimaal 12 karakters met een combinatie van letters, cijfers en speciale tekens.
- Gebruik wachtwoordzinnen of een wachtwoordbeheerder voor eenvoudig en veilig wachtwoordbeheer.
- Schakel waar mogelijk tweestapsverificatie (2FA) in voor uw accounts om een extra beveiligingslaag toe te voegen.
- Hergebruik uw wachtwoord niet.

Antivirus/firewall

- Gebruik firewalls om inkomend en uitgaand netwerkverkeer te controleren en ongeautoriseerde toegang te blokkeren.
- Gebruik betrouwbare anti-malware en antivirustools om schadelijke software te detecteren en verwijderen.
- Scan een gedownload bestand op virussen.
- Laat een virusscanner automatisch een USB-stick scannen.

Applicaties

- Maak geen gebruik van privé-applicaties voor zakelijke doeleinden.
- Houd uw besturingssysteem, applicaties en antivirussoftware up-to-date om beveiligingskwetsbaarheden te patchen.
- Gebruik geen fileshare-applicaties voor uitwisseling van gegevens.
- Beperk de toegang van gebruikers tot gegevens en systemen. Verleen alleen toegang aan degenen die deze nodig hebben om hun werk uit te voeren.
- Beoordeel en monitor de beveiligingspraktijken van derde partij leveranciers die toegang hebben tot uw gegevens of systemen.

Back-ups

- Maak regelmatig back-ups van uw belangrijke bestanden.
- Zorg voor meerdere back-ups op verschillende locaties.
- Test een back-up op betrouwbaarheid.
- Maak een offline back-up.

Social engineering

- Geef nooit een gebruikersnaam of wachtwoord aan een vreemde.
- Verschaf nooit zomaar uw identiteit aan een vreemde.
- Vraag aan een onbekende de reden van het bezoek.

Meer informatie

Neem voor meer informatie contact op met onze IT & Cybersecurity consultant.

Brechtje Brugman-Dekkers
Manager IT Advies
E. B.Brugman@vanoers.nl
T. +31 (0)6 82 04 64 65