WHITEPAPER

Security in het tijdperk van de digitale transformatie

20 BEVEILIGINGSTIPS VOOR DIGITAL ENTERPRISES

TechData

Security in het tijdperk van de digitale transformatie

20 BEVEILIGINGSTIPS VOOR DIGITAL ENTERPRISES

De digitale transformatie biedt bedrijven mogelijkheden om de concurrentiepositie te verbeteren. Maar er zijn ook zorgen over de inzet van nieuwe technologieën. Hoe maken ze veilig gebruik van bijvoorbeeld de cloud, het Internet of Things en data-analytics? In deze white paper geeft Tech Data de antwoorden.

Digitalisering en security

Steeds meer bedrijven mogen zich een 'digital enterprise' noemen. Bij een onderzoek van branchevereniging Nederland ICT gaf bijna de helft van de ondervraagde bedrijven aan dat ICT erg belangrijk is voor de corebusiness van de eigen organisatie. Deze bedrijven zetten technologie in om hun concurrentiepositie te verbeteren.

Dat doen ze bijvoorbeeld door werknemers efficiënter te laten werken. Die zijn niet meer gebonden aan een vaste werkplek, maar halen onderweg data en applicaties uit de cloud. Via het Internet of Things verzamelen digital enterprises data van uiteenlopende sensoren. Analyses van die data leiden tot slimme inzichten, bijvoorbeeld om de bedrijfsvoering efficiënter in te richten. Of om beter te kunnen voldoen aan de eisen en verwachtingen van afnemers en gebruikers van producten en diensten.

Daar staat tegenover dat cybercriminelen steeds meer mogelijkheden krijgen om bij bedrijven binnen te dringen en data te stelen. Gevoelige gegevens bevinden zich bijvoorbeeld niet meer alleen binnen het eigen, lokale bedrijfsnetwerk, maar ook in de cloud en op de apparaten van medewerkers. De (mogelijk onveilige) devices die samen het Internet of Things vormen, kunnen ze gebruiken als springplank naar het interne netwerk. En wie toegang heeft tot de data-analyticsomgeving van een organisatie heeft toegang tot een enorme verzameling waardevolle gegevens.

Het 'aanvalsoppervlak' is door digitalisering groter geworden. Hoe kunnen bedrijven zich hiertegen wapenen? We bespreken hoe u het gebruik van cloud, data-analytics, Internet of Things en het onderliggende netwerk veiliger kunt maken.

Cloud

Optimale beveiliging van data en bedrijfssystemen is cruciaal. Of ze nu binnen de muren van het bedrijfspand staan, of in de cloud. Waar moet u precies rekening mee houden als het gaat om databeveiliging in de cloud? 5 belangrijke aandachtspunten:

1 Selecteer de cloudprovider doelbewust

Een organisatie mag verwachten dat de provider strenge securitymaatregelen treft. Neem dat echter nooit als vanzelfsprekend aan. Laat u goed informeren over de toegangscontroles die een leverancier hanteert en over hoe de security is ingeregeld. Controleer bovendien of een cloudprovider de juiste securitycertificeringen kan overleggen.

2 Neem zelf maatregelen

Goede securityvoorzieningen bij uw cloudprovider ontslaan u niet van een eigen verantwoordelijkheid over de veiligheid van de data. Denk aan het versleutelen van data, het beveiligen van uw verbindingen met de cloud, en het hanteren van een strikt wachtwoordbeleid. Lijdt uw cloudprovider dataverlies, dan is het cruciaal dat u kunt terugvallen op een back-up.

3 Classificeer data

Niet alle data zijn geschikt voor opslag in de cloud. Het is daarom belangrijk uw data te classificeren. Hiermee bepaalt u welke gegevens u zonder problemen in de cloud kunt plaatsen, en voor welke data aanvullende beveiligingsmaatregelen noodzakelijk zijn.

4 Kies de opslaglocatie zorgvuldig

Plaatst u data in de cloud, dan komen deze terecht in een datacenter. Voor een goede security en compliance met de privacywetgeving kan de fysieke locatie van dat datacenter van belang zijn. Grote aanbieders als Microsoft delen hun cloudopslagdiensten in zogeheten regio's in. Daarmee kunnen ze de garantie geven dat u controle over de fysieke opslaglocatie houdt.

5 Betrek uw IT-afdeling vanaf het begin erbij

Het is belangrijk uw IT-team al vanaf het eerste begin te betrekken bij de migratie naar de cloud. De experts in dit team beschikken over de kennis en het inzicht om risico's goed in te schatten. Bekijk samen met hen hoe data nu on-premises zijn beveiligd, en hoe toegangsbeheer is geregeld. Onderzoek vervolgens hoe en of deze aanpak en het beoogde securityniveau ook in de cloud nog steeds mogelijk zijn, zodat uw data ook daar in veilige handen zijn.

Internet of Things

Over de voordelen van het Internet of Things zijn talloze artikelen geschreven. Minder bekend zijn de gevolgen van een IoT-netwerk voor de veiligheid van uw bedrijfsdata. IoT-apparaten zijn niet zelden een rijke bron van waardevolle informatie, ook voor cybercriminelen. En als deze apparaten op een kier staan, ligt er feitelijk een rode loper naar de rest van de systemen en gegevens. Welke maatregelen kunt u nemen om een 'IoT-hack' te voorkomen? We lichten er vijf uit:

1 **Kies IoT-apparaten zorgvuldig**
Goed vooronderzoek is in alle gevallen verstandig. Beschikt een apparaat bijvoorbeeld over tweefactor-authenticatie? Brengt de fabrikant regelmatig veiligheidsupdates uit? Welke communicatieprotocollen zijn in gebruik? Controleer bovendien of de devices data versleuteld opslaan. Kies voor bedrijven die zich op het vlak van security hebben bewezen, en probeer het zogenaamd 'consumenten-IoT' buiten de deur te houden.

2 **Voer een grondige inventarisatie uit**
Een veilig IoT-netwerk begint bij een goed inzicht in de assets. Welke IoT-devices zijn in gebruik, wat is hun serienummer, welke firmwareversie draait erop? Een nauwgezette administratie voorkomt dat apparaten onder de radar blijven en ongemerkt voor onveilige situaties zorgen.

3 **Update de firmware regelmatig**
De firmware van IoT-apparaten kent net als andere software bugs en kwetsbaarheden. Deugdelijke fabrikanten voorzien hun devices regelmatig van firmware-updates, zodat het risico op misbruik van bugs tot een minimum beperkt blijft. Het is zaak deze updates zo snel mogelijk na release te installeren.

4 **Hanteer een strikt wachtwoordbeleid.**
Wachtwoorden vormen de eerste verdedigingslinie tegen digitale inbraak op IoT-apparaten. Een sterk wachtwoord is daarom een noodzakelijke basismaatregel. Hanteer bovendien voor ieder device een ander wachtwoord, en gebruik waar mogelijk tweefactor-authenticatie.

5 **Test de bestendigheid van het IoT-netwerk**
Een pentest kan eventuele kwetsbaarheden in het IoT-netwerk boven water halen. Bij een dergelijke test kruipen gespecialiseerde experts in de huid van een hacker. Afhankelijk van de scope en gekozen delen van de test proberen ze data te stelen en/of op de IoT-apparaten in te breken. Met de testbevindingen kunt u maatregelen nemen voordat 'echte' cybercriminelen u voor zijn.

Data-analytics

Een data-analyticsoplossing biedt toegang tot systemen vol gevoelige, waardevolle data. Beveiliging van een dergelijke omgeving is cruciaal. Data kunnen uitlekken en zo terechtkomen bij de concurrentie. Cybercriminelen kunnen op de omgeving inbreken en de gestolen data doorverkopen op het dark web. Daarnaast verplicht privacywetgeving u tot een goede zorg over opgeslagen persoonsgegevens. Waar moet u op letten bij de selectie van een data-analyticsprovider?

1 Kies een betrouwbare provider

Security is nauwelijks een kernactiviteit voor de meeste organisaties. Toch is het een belangrijk aandachtspunt voor wie aan de slag wil met analytics. Wie zeker wil zijn dat zowel de data als de analytics-oplossing voldoende zijn beveiligd, kiest het beste voor een oplossing van een bewezen provider, zoals Amazon Web Services, Hitachi, Microsoft of Oracle.

2 Controleer de veiligheidsprocedures

Veiligheidsprocedures verkleinen de kans op een geslaagde cyberaanval. Wie een provider kiest, doet er goed aan te controleren welke procedures deze hanteert. Een bekende methode is bijvoorbeeld DREAD, een procedure die beveiligingsproblemen in systemen opspoort. Ook regelmatige audits en pentesten door externe, onafhankelijke partijen zijn een goed teken.

3 Richt de toegangsbeveiliging in

Net zo'n belangrijk aandachtspunt is hoe de toegang tot de oplossing is geregeld. Uiteraard mogen alleen bevoegde gebruikers erbij komen, en dan enkel met de hoogst noodzakelijke rechten. Een reguliere gebruiker zou bijvoorbeeld geen databronnen mogen verwijderen of toevoegen. Ook is het zaak dat een gebruiker slechts die informatie krijgt te zien die strikt noodzakelijk is voor zijn of haar functie. Een goede analytics-oplossing biedt een fijnmazig systeem voor het instellen van rechten per individuele gebruiker.

4 Besteed aandacht aan gegevensbeveiliging

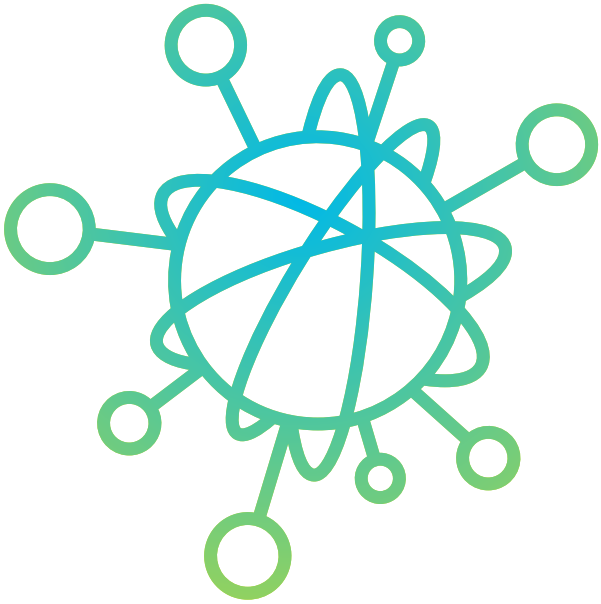
Ten slotte is de manier waarop een provider databeveiliging toepast een doorslaggevende factor. Een belangrijk aandachtspunt is bijvoorbeeld of de datastroom tussen de gegevensbronnen en de software wordt versleuteld. Ook is het goed om na te gaan op welke wijze de software de data beschermt tijdens het analytics-proces.

5 Train de gebruikers

Soms vormen niet de hardware en software het grootste beveiligingsrisico, maar eerder de mensen die ermee werken. Cloudanalytics maakt data overal beschikbaar, dus ook via openbare wifi en in de trein waar meelezende ogen zijn. De gebruikers moeten zich hier bewust van zijn. Investeer daarom in een securitytraining voor alle medewerkers.

Netwerken

Als u hackers zo min mogelijk bewegingsruimte wilt geven op uw bedrijfsnetwerk, zijn een veilig ontwerp en slimme instellingen essentieel. Een slim netwerkontwerp maakt het voor hackers lastiger om binnen te komen en data te ontfutselen. Deze 5 aandachtspunten zijn goed om in ogenschouw te nemen:



1 **Zorg voor fysieke veiligheidsmaatregelen**
Fysieke beveiliging is een noodzakelijke voorwaarde voor goede netwerkbeveiliging. Zorg voor algemene gebouwbeveiliging zoals toegangscontrole. Daarnaast is het belangrijk dat de fysieke netwerkonderdelen als switches, access points, firewalls en bekabeling zoveel mogelijk uit het zicht, aan het plafond en/of achter slot en grendel zijn geplaatst.

2 **Segmenteer het netwerk**
Het is belangrijk de bewegingsruimte van indringers die eenmaal 'voorbij de voordeur zijn' te beperken. Een goede maatregel is segmentatie van het netwerk. Met behulp van VLAN's verdeelt u het netwerk in zones. Deze zones zijn onderling begrensd. Zo kunt u een virtueel netwerk toekennen aan bijvoorbeeld alle opslagservers of bepaalde afdelingen.

3 **Pas ook op het bekabelde netwerk versleuteling toe**
Vrijwel alle organisaties versleutelen hun wifinetwerk. Minder gebruikelijk is de versleuteling van de bekabelde verbinding. Dat is ingewikkelder dan wifiversleuteling en vereist de toepassing van technieken als IPsec of interne VPN-tunnels. Toch kan het de moeite waard zijn. Komt een hacker binnen op een bekabeld, versleuteld netwerk, dan kan hij of zij geen data verzenden, ontvangen of onderscheppen.

4 **Beperk de rechten van wifigebruikers**
Wifinetwerken zijn van nature kwetsbare toegangspoorten tot het bedrijfsnetwerk. De kans op een hack verkleint u door via deze weg alleen internettoegang toe te staan. Eventueel kunt draadloze communicatie met het bedrijfsnetwerk toestaan via een VPN-verbinding.

5 **Leg uitgebreide logs aan**
Informatie is een belangrijk wapen tegen hackers. Daarom is het belangrijk zoveel mogelijk informatie over het netwerkverkeer en -gebruik vast te leggen in logs. Logs stoppen aanvallers weliswaar niet direct, maar uit de zee aan informatie kunnen intelligente systemen op handen zijnde aanvallen wel detecteren. Een SIEM (security information and event management)-oplossing kan de verzamelde logs eventueel met elkaar correleren om zo het totale dreigingsbeeld scherp te krijgen.

Passende antwoorden

Het ontwerpen van een veilig netwerk is niet gemakkelijk. Hetzelfde geldt voor de beveiliging van het IoT en data in de cloud. Herstelwerkzaamheden na een cyberaanval zijn echter vele malen ingewikkelder.

Door een aantal basismaatregelen in acht te nemen, kunt u veel ellende voorkomen. Maar digital enterprises zijn er natuurlijk nog niet met het opvolgen van de twintig tips in deze white paper. Zo hebben we het nog niet gehad over het beveiligen van mobiele devices, applicaties en databases.

Wilt u daar meer over weten? Tech Data helpt u graag met het vinden van passende antwoorden op de securityuitdagingen in het digitale tijdperk.

Contactgegevens
Tech Data Nederland B.V.
Tolnasingel 2
2411 PV Bodegraven
T. +31 (0) 88 133 40 00
M. info@techdata.nl