SECURITY EN GDPR/AVG

ALS CYBERCRIME KINDERSPEL WORDT

Hoe help je bedrijven zich te weren tegen nieuwe bedreigingen?

2018 – hét securityjaar bij uitstek – was nog maar net begonnen of een aantal nationale banken, grote websites en de Belastingdienst werden slachtoffer van een DDoS-aanval. In eerste instantie werd gedacht aan professionele hackers uit het buitenland, maar toen het een jongen bleek te zijn die pas net oud genoeg was om een biertje te kopen, was de ontluistering groot. Want als een hobbyist al zo veel schade kan aanrichten, wat staat ons dan te wachten?

door: Sander Nieuwstraten, Business Unit Manager Networking & Security Arrow ECS

De aanvallen van de Brabantse tiener werden breed uitgemeten in het nieuws, maar de praktijk leert dat de echt gevaarlijke aanvallen veelal onder de radar blijven. Arrow-resellers die MSSP (Managed Security Service Provider) diensten leveren, zien dat hun klanten continu onder vuur liggen van professionele hackers met soms meer dan duizenden attacks per dag. Deze cybercriminelen zorgen dat ze zo lang mogelijk onzichtbaar blijven zodat ze hun opbrengst kunnen maximaliseren waarbij ze grote schade aanrichten.

Fake data en discotheek-authenticatie

Security is een wapenwedloop geworden tussen cybercriminelen en security-experts waarbij vendoren van security-oplossingen op iedere nieuwe aanval zo snel mogelijk een oplossing of verdediging moeten zien te bieden. Er komen dan ook steeds meer nieuwe fabrikanten bij die interactieve technieken op de markt brengen.

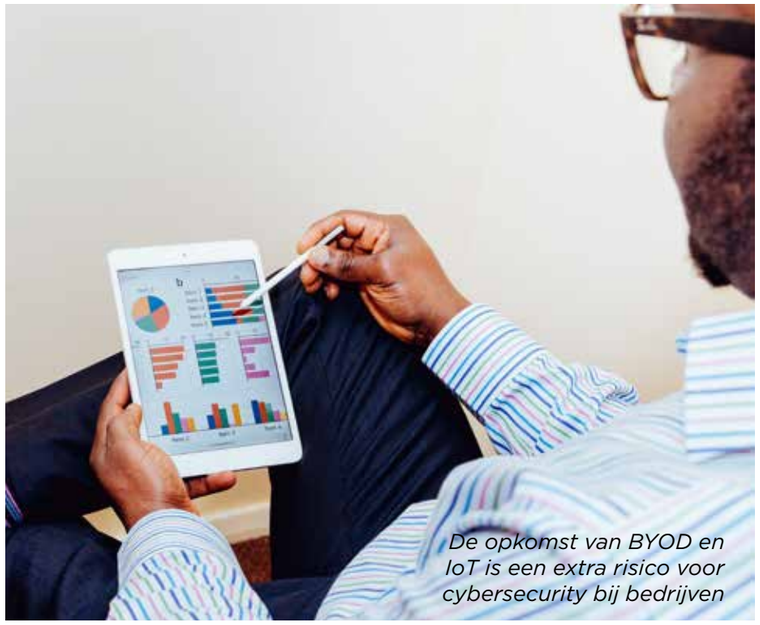
Was het een aantal jaar geleden nog voldoende om reactief te werk te gaan, inmiddels gaan de ontwikkelingen zo snel dat vendoren proactief moeten zijn. Ze moeten dreigingen, maar ook verdachte activiteiten kunnen herkennen en die direct het hoofd kunnen bieden. Next generation security-oplossingen gebruiken diepgravende analyses en machine learning om bestanden en gedragingen op het bedrijfsnetwerk te analyseren en monitoren. Op die manier identificeren en blokkeren ze bekende en onbekende malware, maar ook niet-malware en unwanted software. De dreiging komt lang niet altijd van buitenaf, vandaar dat ook user behavior nauwlettend in de gaten moet worden gehouden.

Een relatief nieuwe strategie die bij steeds meer eindgebruikers wordt ingezet, is het toevoegen van fake data aan databases. Wanneer deze gegevens – die geen nut of betekenis hebben – worden aangesproken, is meteen duidelijk dat er een niet-geautoriseerd persoon of programma op het netwerk zit. Het is bijna een soort omgekeerd phishing. Verder is het invoeren van een streng authenticatie-beleid weer heel actueel. Net zoals het deurbeleid bij een discotheek: 'Ik vertrouw niemand tot ik je heb toegelaten.'

> Gelukkig zijn er manieren om een veilig IoT-beleid te hanteren

Een veilige IoT-strategie

Door recente ontwikkelingen als BYOD (Bring Your Own Device) en de opkomst van Internet of Things is het aanscherpen van het deurbeleid voor je netwerk zeker geen overbodige luxe geworden. Zelfs onschuldig speelgoed dat gebruikmaakt van je netwerk, kan al een ingang zijn voor kwaadwillenden, maar daar denkt niemand meteen over na.



De opkomst van BYOD en IoT is een extra risico voor cybersecurity bij bedrijven

> Het aanscherpen van het deurbeleid voor je netwerk is zeker geen overbodige luxe

IoT kun je niet buiten de deur houden, zeker niet nu steeds meer bedrijven het zelf inzetten en nodig hebben voor hun bedrijfsvoering en om concurrerend te blijven. Gelukkig zijn er manieren om een veilig IoT-beleid te hanteren. Deze 7 beginselen kunnen daarbij helpen.

1. **Authenticatie:** Iedereen die toegang tot het netwerk vraagt, moet worden geautoriseerd. Dit moet een essentieel onderdeel van de IT-infrastructuurstrategie zijn, waarbij het toegangsbeheer op rollen gebaseerd is en bij wordt gehouden wie er deel mag nemen aan het netwerk en wanneer die accounts worden gebruikt.
2. **Encryptie:** Codering is vereist om controle te kunnen houden over de data die wordt gedeeld van devices naar centrale applicaties. De snelheid van het dataverkeer mag hier echter niet onder lijden.
3. **Transmissie:** Het verkeer van gegevens tussen apparaten en naar het netwerk moet worden overwogen. Hebben apparaten een bekabelde verbinding met het netwerk of verloopt dit draadloos? Voor logistieke bedrijven kan het nodig zijn gebruik te maken van telecomnetwerken om voertuigen te volgen. Data-overdracht, of dit nu bekabeld of draadloos is, moet beveiligd zijn en moet eenvoudig kunnen worden geüpgraded om aan de nieuwste communicatieprotocollen te voldoen.
4. **Sabotagebeveiliging:** Deze stap zorgt ervoor dat apparatuur wordt gemonitord en gecontroleerd om te zien of er niet mee is geknoeid. Dit kan door een combinatie van mechanische, hardware- en softwarematige sabotagedetectie.
5. **Gegevensopslag:** Alle data-opslag moet veilig zijn. Gegevens die in de edge worden opgeslagen kunnen bijvoorbeeld ook kritieke systeemgegevens bevatten, zoals besturingssoftware. Ook geheugen-uitbreiding – wat zeer waarschijnlijk moet gebeuren tijdens de levenscyclus van apparatuur – moet op een veilige manier worden gedaan. Maar ook de centrale dataset heeft bescherming nodig omdat dit een kritisch bedrijfsmiddel is.
6. **Draadloze upgrade:** Industriële apparatuur kan variëren van levensduur, maar meestal zal de software tussentijds moeten worden geüpdatet. Een IoT-systeem moet op een veilige manier over-the-air security-updates kunnen krijgen.
7. **Segmentatie:** De meeste bedrijven hebben een platte netwerkstructuur en elke fout in een apparaat kan zich door het hele netwerk verspreiden en de performance beïnvloeden. Segmentatie minimaliseert het effect van een aanval, mocht die onverhoopt plaatsvinden.

Ontzorgen met MSSP

Privacywetgeving wordt steeds strenger en cybercriminaliteit steeds agressiever. De bedrijfsrisico's worden groter en er moet steeds meer geld, tijd en aandacht in security worden geïnvesteerd. Geen wonder dat middelgrote bedrijven en enterprises deze activiteit vaker uitbesteden aan specialisten zodat zij zich weer met hun core business bezig kunnen houden.

Resellers migreren steeds vaker naar MSSP's die op afstand de security kunnen monitoren, beheren en patches kunnen uitrollen. Eindklanten betalen een vast bedrag en krijgen periodiek een overzicht van de gedane activiteiten. Verder hebben ze er geen omkijken naar en zijn ze verzekerd van het securitypakket dat zij nodig hebben. Beveiliging bestaat immers al lang niet meer uit één oplossing, maar is altijd een pakket van meerdere producten die samen aansluiten bij de specifieke situatie van de eindklant.

Als het om security gaat, kun je op dit moment nooit alle risico's en bedreigingen voorkomen. Maar met gezond verstand en de juiste leveranciers, kunnen organisaties heel ver komen. «