WIRELESS LOGIC **STUDIE**

Verhoogde risico's van IoT-beveiliging:

bent u voorbereid?

wirelesslogic.com/nl

Inleiding

Auto's, camerabeveiliging en slimme horloges. Ze kunnen allemaal met het internet zijn verbonden om online gegevens te verzenden. Op deze manier kan een horloge locatiegegevens verzamelen als u 's ochtends gaat hardlopen.

Of gegevens realtime analyseren, zoals uw hartslag. Dit kunt u in veel sectoren terugzien. Een voorbeeld is een hartimplantaat waarmee een arts een patiënt op afstand in de gaten kan houden. Of sensoren die in de landbouw worden gebruikt om bodemvochtigheid nauwkeurig vast te stellen.

Al deze toepassingen worden Internet of Things (IoT)-oplossingen genoemd. Dit zijn systemen waarbij verbonden apparaten gegevens verzamelen, uitwisselen en analyseren via het internet.
Ze kunnen het dagelijks leven efficiënter maken, maar dat neemt niet weg dat er veel risico's zijn. Onlangs was nog in het nieuws dat stoplichten relatief makkelijk te hacken zijn. Dit is ook een voorbeeld van een IoT-oplossing, want stoplichten gebruiken sensoren om verkeer te detecteren. Wat als een buitenstaander alle stoplichten tegelijkertijd op groen zou zetten? De gevolgen van een aanval kunnen ernstig zijn. IoT-apparaten hebben vaak toegang tot gevoelige gegevens – denk maar aan het voorbeeld van het hartimplantaat in het ziekenhuis -, wat het risico op datadiefstal vergroot. Dit leidt mogelijk tot hevige privacy-inbreuken. In industriële omgevingen kan een hack leiden tot productieverlies.

In verschillende vakgebieden zijn IoT-oplossingen in opkomst, aangedreven door technologische vooruitgang. We zijn in toenemende mate afhankelijk van IoT en dit zorgt ervoor dat beveiligingsrisico's een steeds grotere rol spelen. Door de opkomst van AI wordt hacken eenvoudiger. Het is niet langer de vraag of u gehackt wordt, maar wanneer. En toch hebben veel apparaten nog zwakke wachtwoorden. Of maken ze gebruik van verouderde software met alle bijbehorende kwetsbaarheden. Terwijl beveiligingsrisico's steeds prominenter worden.

Daarom heeft Wireless Logic onderzoek laten doen onder 215 respondenten om in kaart te brengen hoe organisaties aankijken tegen IoT-connectiviteit. Het onderzoek is gehouden onder C-level en strategische managers. De resultaten kunt u gebruiken om uw eigen IoT-beveiliging onder de loep te nemen. Tegelijkertijd kunt u inzichten uit het onderzoek gebruiken als een spiegel. Hoe bewust bent u van de risico's die u zélf loopt? Tot slot komen diensten aan bod die bedrijven kunnen helpen op het gebied van IoT-beveiliging.

Het grote belang van databeveiliging

Bij het beveiligen van IoT-apparaten komt veel kijken.

Een grote uitdaging waar u tegenaan loopt is de variëteit aan apparaten en technologieën. Als apparaten op hetzelfde besturingssysteem draaien, is het nu eenmaal eenvoudiger om uniforme beveiligingsmaatregelen toe te passen.

Bovendien heeft elk apparaat andere kwetsbaarheden. Dit hangt niet alleen af van het besturingssysteem, maar ook van de hardware. Sommige slimme sensoren, die regelmatig in ziekenhuizen worden gebruikt, hebben bijvoorbeeld een gering geheugen. Dit maakt de mogelijke beveiligingsmaatregelen beperkt. Bij zonnepanelen worden soortgelijke sensoren gebruikt om vast te stellen wanneer onderhoud nodig is. Daarnaast zijn de grote verschillen in schaal en functie van IoT-apparaten een complicerende factor.

Implementatie en beheer

Tegen welke uitdagingen u ook aanloopt, er zijn geen wereldwijde standaarden voor IoT-beveiliging. Sommige apparaten hanteren dus mogelijk onveilige standaarden. Dit hangt mede af van hoe belangrijk organisaties IoT-beveiliging achten. Van de respondenten geeft meer dan de helft (53%) aan databeveiliging als één van de belangrijkste uitdagingen op het gebied van implementatie en beheer van IoT in hun organisatie te zien. Een vijfde (21%) zit pas in de beginfase op het gebied van IoT.

De belangrijkste uitdagingen bij de implementatie en het beheer van IoT in de organisatie

Databeveiliging	53%
Integratie met bestaande systemen	44%
Technische complexiteit	36%
Betrouwbaarheid en beschikbaarheid van IoT-apparaten	32%
Hoge investeringskosten	31%
Gebrek aan gespecialiseerde kennis	28%
De mogelijkheid van IoT-oplossingen om mee te groeien met het bedrijf	23%
Gebrek aan betrouwbare leveranciers en partners	16%
Anders	0,9%

Afhankelijkheid van IoT

Zoals reeds kort uiteengezet, kunnen datalekken van IoT-apparaten ernstige gevolgen hebben. IoT-apparaten zijn namelijk ook zonnepanelen, laadpalen, alarmsystemen, sluizen en bruggen. Kritieke systemen als energiecentrales kunnen worden gehackt. Of intellectueel eigendom wordt geschonden. Om daadwerkelijk inzicht te krijgen in het bewustzijn van de afhankelijkheid van IoT voor bedrijfsprocessen, hebben we daar specifiek naar gevraagd. Meer dan de helft van de respondenten geeft aan zich hier bewust van te zijn en dat een grootschalige cyberaanval op IoT-apparaten zou zorgen voor een ernstige verstoring, zoals het stilleggen van energievoorzieningen of transportnetwerken.

De overheid

Dit benadrukt het belang van databeveiliging van IoT-systemen, maar de rol van de overheid mogen we evenmin onderschatten. De helft van de respondenten geeft aan dat IoT-beveiliging vanuit overheden en regelgevende instanties ontoereikend is om grote cyberaanvallen op vitale infrastructuren te voorkomen. Dit is zorgwekkend met het oog op de grote gevolgen van een datalek.

"Een groot aantal (68%) is van mening dat IoT-beveiliging in de organisatie in de kinderschoenen staat."

Bewustzijn over de risico's

Ondertussen vertrouwt meer dan de helft (53%) van de respondenten op de beveiliging van hun connectiviteitspartner en zien ze geen noodzaak voor extra IoT-beveiligingsmaatregelen.

Dit geldt voor grofweg een derde (35%) van de organisaties die in de beginfase van IoT zitten en de helft (52%) van de organisaties die enkele toepassingen van IoT geïntegreerd hebben. Twee derde (66%) van de organisaties die geavanceerd zijn op het gebied van IoT was het hiermee eens. Zeven tiende (70%) van de organisaties die leidend zijn op het gebied van IoT, gaf te kennen zich in deze stelling te kunnen vinden. Het lijkt erop dat de cijfers in schril contrast staan met de hoge risico's die verbonden zijn aan datalekken in met name vitale infrastructuren. Een voorlopige conclusie is dat het bewustzijn niet strookt met de hoogte van de risico's.

IoT-beveiliging in de kinderschoenen

Meer dan de helft (55%) van de respondenten noemt cybersecurity de aanvullende dienst die het meest toegevoegde waarde zou hebben. Een vergelijkbaar percentage (53%) noemt databeveiliging de belangrijkste uitdaging bij de implementatie en het beheer van IoT in hun organisatie. Een nog groter aantal (68%) is van mening dat IoT-beveiliging in de organisatie in de kinderschoenen staat. Er is een grote discrepantie tussen het zien van noodzaak voor extra IoT-beveiligingsmaatregelen en waar organisaties staan op het gebied van IoT-beveiliging.

De toekomst tegemoet

Dat neemt niet weg dat meer dan de helft (53%) IoT-oplossingen als de toekomst ziet. Bijna de helft (44%) denkt zelfs dat IoT binnen vijf jaar een kernonderdeel van processen is. Dit komt overeen met het zojuist geschetste beeld. Respondenten zien het belang van IoT-oplossingen voor de bedrijfsvoering. Een overtuigende meerderheid (86%) geeft aan meer in IoT-oplossingen te willen investeren in de toekomst, maar een groot deel hiervan (38%) wordt vooralsnog belemmerd door een gebrek aan interne expertise. Technologie wordt steeds complexer. Dit kunnen medewerkers moeilijk bijhouden, wat leidt tot krapte op de arbeidsmarkt.

Bewustzijn niet op overeenkomstig niveau

Respondenten erkennen dus dat IoT-beveiliging belangrijk is, maar het bewustzijn is (nog) niet op overeenkomstig niveau. Een opvallend resultaat is dat meer dan de helft (53%) aangeeft dat hun organisatie vol inzet op IoT-beveiliging. Zoals al aangestipt, vertrouwt eenzelfde percentage erop dat hun connectiviteitsprovider hun systemen voldoende heeft beveiligd. Zouden extra IoT-beveiligingsmaatregelen dan ook uitblijven?

Als organisaties niet op tijd overstappen naar nieuwe technologieën, kan dit hun kwetsbaarheid vergroten. Organisaties die afhankelijk zijn van 2G/3G-netwerken kunnen problemen ondervinden als ze daar onvoldoende rekening mee houden; niet alle apparaten die afhankelijk zijn van 2G/3G-netwerken kunnen eenvoudig worden geüpgraded naar 4G of 5G. Dit kan leiden tot vertragingen van bedrijfsprocessen of zelfs datalekken omdat oude hardware niet voldoet aan moderne beveiligingsstandaarden. Bijna twee vijfde (38%) van de respondenten staat niet stil bij het naderende einde van het 2G/3G-tijdperk. Dit maakt ze mogelijk kwetsbaarder voor onverwachte risico's. Daar staat tegenover dat een derde (32%) het niet eens is met deze stelling.

Bijna twee vijfde

(38%)

van de respondenten staat niet stil bij het naderende einde van het 2G/3G-tijdperk.

"Er is een groot contrast tussen de grootte van de risico's en de benadering van organisaties van hun IoT-beveiliging."

Benaderingen voor IoT-beveiliging

Meer dan de helft (58%) heeft netwerk- en databeveiliging (VPN-gebruik, direct connect, netwerksegmentatie, firewalls, private netwerken) geïmplementeerd voor IoT-apparaten en -netwerken.

Een zorgwekkend grote groep heeft deze keuzeoptie dus niet ingevuld. Er is een groot contrast tussen de grootte van de risico's en de benadering van organisaties van hun IoT-beveiliging. Minder dan de helft (44%) heeft procedures als back-up en herstel als beveiligingsmaatregel, identiteits-en toegangsbeheer (43%) of apparaatbeveiliging als IMEI-lock, multifactor-authenticatie, firmware-updates of secure boots (41%).

Welke beveiligingsmaatregelen hebben organisaties geïmplementeerd voor IoT-apparaten en – netwerken?

Netwerk- en databeveiliging	58%
Procedures	44%
Identiteits- en toegangsbeheer	43%
Apparaatbeveiliging	41%
Monitoring en detectie	39%
Supply chain beveiliging	30%
Compliance en incident response	27%
Geavanceerde technologieën	25%
Anders	0,9%

Proactieve aanpak

Ondertussen geeft een ruime meerderheid van de respondenten (61%) aan proactief te zijn in het identificeren en aanpakken van IoT-beveiligingsrisico's. Het lijkt er dus op dat er weinig bewustzijn bestaat over IoT-beveiliging bij organisaties. Het blijft een uitdaging om organisaties te overtuigen van de potentiële gevaren. Het niveau van bewustzijn varieert afhankelijk van de gevraagde partijen, maar dat het onderwerp veel in het nieuws komt, en er bovendien campagnes en trainingen bestaan om het bewustzijn te vergroten, zijn positieve ontwikkelingen.

Conclusie

Bij Wireless Logic onderkennen we dat een betrouwbare connectiviteitspartner essentieel is in een steeds meer verbonden wereld.

Uit ons onderzoek blijkt dat veiligheid en compliance voor 52% van de respondenten doorslaggevende factoren zijn in hun bedrijfsvoering. Tegelijkertijd wordt de noodzaak van aanvullende IoT-beveiligingsmaatregelen vaak onderschat. Dit roept een belangrijke vraag op: wat gebeurt er als een alarmsysteem of kritieke infrastructuur, zoals een sluis, wordt gehackt? Het effectief beveiligen van IoT vereist een volwassen aanpak, continu onderhoud en gespecialiseerde expertise.

IoT biedt organisaties ongekende mogelijkheden, maar gaat ook gepaard met aanzienlijke risico's, zoals ongeoorloofde toegang, ransomware en apparaatspoofing. Zonder een solide beveiligingsstrategie kunnen deze bedreigingen leiden tot grote reputatie- en financiële schade. Daarom biedt Wireless Logic geïntegreerde oplossingen om IoT-beveiliging effectief te verweven in digitale strategieën. Onze aanpak richt zich op end-to-end beveiliging, betrouwbare identificatie en authenticatie, en realtime detectie en respons.

Met een geïntegreerde aanpak, waaronder on-SIM authenticatie, bieden wij robuuste beveiligingsoplossingen die implementaties vereenvoudigen en fouten in productie- en onderhoudsprocessen minimaliseren. Elk apparaat wordt betrouwbaar geïdentificeerd en geauthentiseerd via cloudcertificaten en hardware-identificatie, zoals IMEI, wat het risico op ransomware en fraude aanzienlijk verkleint. Onze monitoringoplossingen detecteren verdachte activiteiten vroegtijdig, waardoor snelle interventies mogelijk zijn en waardevolle inzichten worden verkregen voor proactief risicobeheer. Daarnaast bieden wij oplossingen waarmee u buiten het openbare internet kunt verbinden, wat een extra laag van beveiliging toevoegt en ongeoorloofde toegang verder beperkt.

Wireless Logic is toegewijd aan het leveren van toekomstbestendige, schaalbare beveiligingsoplossingen die voldoen aan internationale normen zoals ETSI EN 303 645. Hiermee helpen wij organisaties niet alleen risico's te beheersen, maar ook efficiëntie en concurrentievoordeel te behalen in een steeds complexere IoT-omgeving.

IoT-beveiliging is geen luxe, maar een noodzaak. Met Wireless Logic als partner kunnen organisaties rekenen op een strategische aanpak en geavanceerde technologieën die de veiligheid van gegevens, apparaten en infrastructuren waarborgen. Wij staan klaar om organisaties te ondersteunen in het realiseren van een veiliger en toekomstbestendig IoT-ecosysteem. Neem contact met ons op voor meer informatie of persoonlijk advies. Samen bouwen we aan een sterke en veilige digitale.

Verantwoording

Het onderzoek is uitgevoerd in de periode van vijftien tot tweeëntwintig oktober in 2024 onder 215 respondenten. Dit waren C-level en strategische managers, werkzaam in een organisatie van 50+ FTE, die op welke manier dan ook binnen de organisatie te maken hebben met IoT-oplossingen.

Certificate Number 19387
ISO 9001, ISO 22301, ISO 27001
ISO 14001, ISO 50001

Nederland

HQ Wireless Logic Benelux
Meerenakkerweg 1A, 5652 AR Eindhoven

Nederland

+31 (0)40 8 489 489
info.bnx@wirelesslogic.com

Andere kantoorlocaties

Oostenrijk	**Italië**
China	**Liechtenstein**
Denemarken	**Noorwegen**
Frankrijk	**Spanje**
Duitsland	**Verenigd Koninkrijk**

wirelesslogic.com/nl