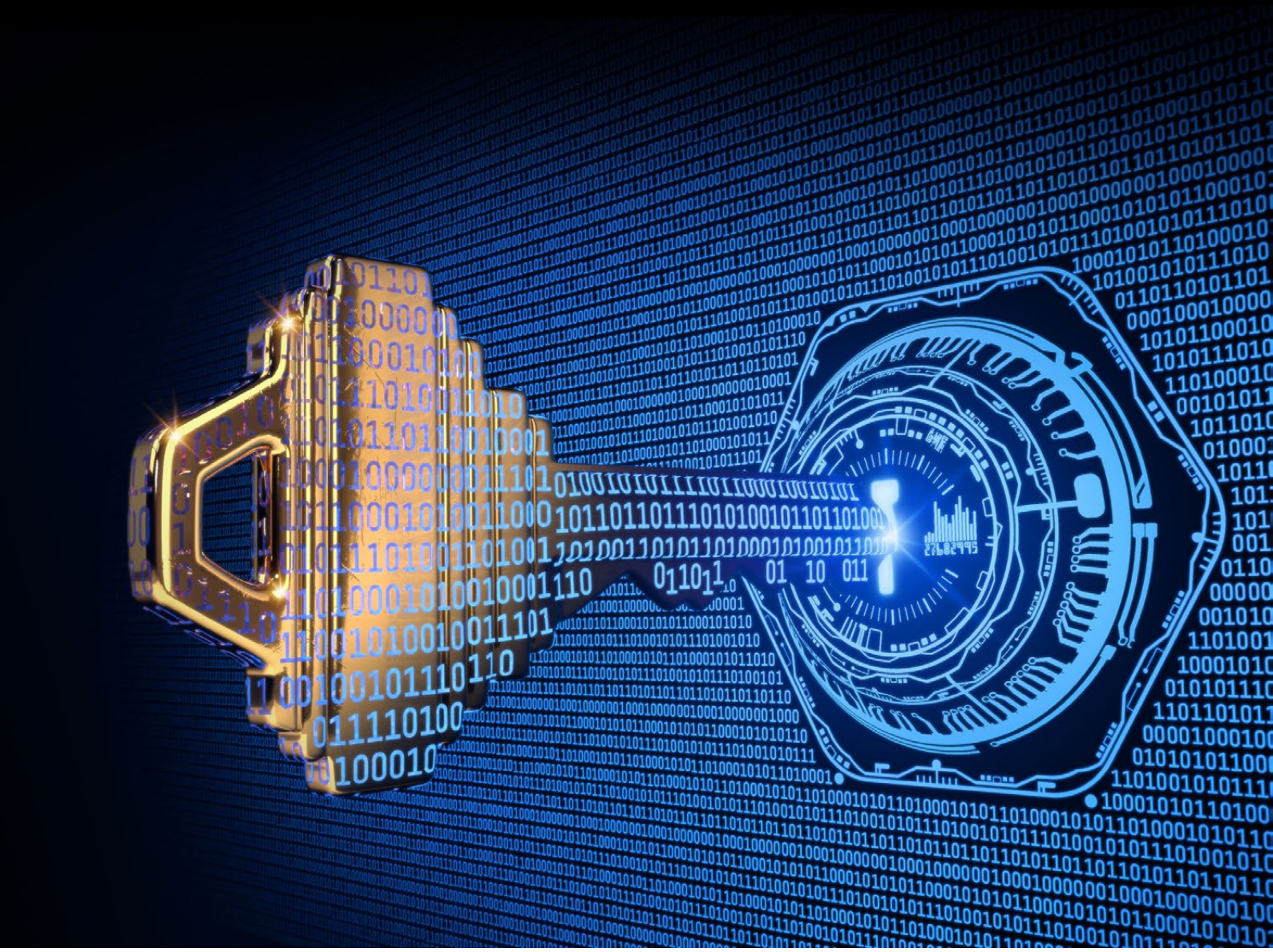
Whitepaper Cyber Security



KNX NATIONAL
THE NETHERLANDS

Inhoudsopgave Whitepaper Cyber Security

Inleiding

Cyber Security start met bewustwording

Installaties in gebouwen, zoals gebouwbeheerssystemen, domotica, klimaatregelingen of beveiligingssystemen, zijn steeds vaker met het internet verbonden. Met name een gebouwbeheerssysteem of een domoticasysteem stuurt meerdere installaties in een gebouw of woning centraal aan en laat deze samenwerken. De afgelopen jaren is gebleken dat installaties die aan internet zijn gekoppeld een aantrekkelijk doelwit vormen voor cybercriminelen.

Op dit moment kunnen professionele bedrijven, zoals installateurs, facility managers of systeem integrators, dankzij internet veel van dit soort installaties op afstand onderhouden, bedienen en bewaken. Ook particulieren beschikken in hun woning steeds vaker over domotica-systemen die zij via internet op afstand met een smartphone of tablet kunnen bedienen. Het is zeer de vraag of al deze partijen zich bewust zijn van de risico's die zij lopen door de koppeling van hun systemen met internet.

Om de problematiek rondom de veiligheid van op afstand bedienbare slimme gebouwen en woningen te 'tackelen' zijn enkele partijen een samenwerking aangegaan. In deze coalitie werken de volgende branche- en kennisorganisaties samen:

- Techniek Nederland, de ondernemersorganisatie voor de installatiebranche en de technische detailhandel.
- FHI/Brancheorganisatie Gebouwautomatisering, de branchevereniging voor gebouwautomatisering.
- KNX Nederland, de vereniging die de internationale standaard voor woning- en gebouwautomatisering in Nederland vertegenwoordigt.
- Wij Techniek, het Opleidingsfonds Technische Installatiebranche.

Dat de gevaren zeer reëel zijn, blijkt uit recent onderzoek. Onder meer het adviesbureau Computest heeft door zogeheten intrusietesten aangetoond dat gebouwbeheerssystemen doelwit kunnen worden van cyberaanvallen. Via een scan lieten zij begin 2019 zien dat veel gebouwautomatiseringssystemen een onbeveiligde koppeling hebben met internet. Toekomstige ontwikkelingen, zoals de energietransitie (aan internet gekoppelde monitoring voor zonnepanelen, energiebeheer, e.d.) slingeren verdere digitalisering aan. Desondanks zijn internetkoppelingen wenselijk of zelfs noodzakelijk voor monitoring en beheer, als we ons er maar bewust van zijn dat dit ook een risico vormt.

Dat betekent dat de bewustwording bij alle partijen in de installatiemarkt, van producent, installateur en systeem integrator tot gebouwbeheerder en eindgebruiker, stevig zal moeten toenemen. Met deze whitepaper helpen wij alle partijen om dat bewustzijn te vergroten. Zodra je je bewust bent dat er een gevaar kan ontstaan en waar die gevaren vandaan kunnen komen, kun je actie ondernemen om deze te elimineren of in elk geval te minimaliseren.

Heb je na het lezen van deze whitepaper nog vragen of opmerkingen, laat het ons weten en neem contact met ons op.

KNX Nederland
Januari 2021

1 Cyber security; een introductie

Hoe kunnen we de kwetsbaarheden minimaliseren die onze digitale wereld en de digitalisering met zich meebrengen?

Cyber security is een relatief nieuwe term en staat, in algemene zin, voor het beschermen van computers, servers, mobiele apparaten, elektronische systemen, netwerken en digitale gegevens tegen schadelijke aanvallen door cyber criminelen. Het wordt ook wel IT-beveiliging genoemd, of beveiliging van elektronische gegevens. Door de inzet van cyber security kunnen we de kwetsbaarheden die onze digitale wereld en de digitalisering met zich meebrengen, minimaliseren. We kunnen er zakelijke omgevingen mee beveiligen, maar ook smart homes en smart buildings, waar diverse apparaten, systemen en diensten met het internet verbonden zijn.

Van computers, websites en digitale besturingssystemen tot en met de talrijke, met het internet verbonden apparaten in woningen, kantoren en fabrieken; in het digitale tijdperk vinden cybercriminelen steeds meer mogelijkheden om deze systemen en de aanwezige data te hacken. Beveiliging van digitale systemen en apparaten in woningen en gebouwen is daarom net zo belangrijk als de beveiliging van je laptop, smartphone of webshop, maar krijgt nog lang niet zo veel aandacht. Niemand wil dat hackers, via toegang tot jouw slimme thermostaat, er achter komen wanneer je op vakantie bent of dat ze via jouw IP-camera al je wifi-inloggegevens achterhalen. Of veel erger, door een aanval op een besturingssysteem een kerncentrale ontregelen. Hoewel ons leven een stuk eenvoudiger en comfortabeler wordt door de vele, met het internet verbonden apparaten en diensten, zetten we zonder goede beveiliging de deur wagenwijd open voor digitale inbrekers. Cyber security is dan ook één van de belangrijkste uitdagingen in onze steeds meer, digitaliserende wereld.

Soorten cyberdreigingen

Er zijn drie soorten cyberdreigingen waartegen cyber security ons kan beschermen: cybercriminaliteit, cyberaanvallen en cyberterrorisme.

1. Cybercriminaliteit zijn aanvallen van criminelen die alleen of georganiseerd systemen aanvallen voor financieel gewin of het veroorzaken van storingen waardoor mensen of bedrijven financieel geraakt worden.
2. De tweede dreigingsvorm, de cyberaanval, is vaak gericht op het verzamelen van informatie via het aangevallen systeem of op het lamleggen van bepaalde systemen waardoor deze niet meer bruikbaar zijn.
3. Van cyberterrorisme is sprake als terroristen via elektronische systemen proberen het vertrouwen en veiligheidsgevoel van het publiek te ondermijnen met als doel angst en paniek zaaien.

Veelgebruikte methoden van cybercriminelen

Er zijn veel verschillende manieren waarop kwaadwillende personen de controle kunnen overnemen bij systemen die op het internet zijn aangesloten. Hieronder staan enkele veelgebruikte methoden die worden ingezet bij cybercriminaliteit, cyberaanvallen en cyberterrorisme.

Virus

Een virus is een klein programma dat de werking van je computer verstoort. Een virus kan gegevens op je computer beschadigen of verwijderen, je e-mailprogramma gebruiken om zichzelf te verspreiden of zelfs je hele harde schijf wissen. Veel virussen worden per e-mail verspreid en zijn vermomd als onschuldige bijlage, zoals een foto of geluidsbestand.

Malware

Malware staat voor ‘malicious software’ (kwaadaardige software) en is een van de meest voorkomende en bekendste vormen van cyberdreiging. Hackers en cybercriminelen ontwikkelen malware met als doel om de werking van (computer)systemen te verstoren of het systeem te beschadigen. Ook malware wordt vaak vermomd als e-mailbijlage of legitieme download, in de hoop dat gebruikers de schadelijke software downloaden. Cybercriminelen gebruiken malware onder andere om hun slachtoffers geld afhandig te maken of om cyberaanvallen met een politiek motief uit te voeren.

Phishing

Als criminelen via e-mail naar informatie ‘hengelen’, noemen we dat phishing. Dit kan via de mail (maar ook via de telefoon) waarbij de afzender vaak betrouwbare instanties lijken te zijn, zoals een bank of creditcardmaatschappij, die dan vragen om bijvoorbeeld inloggegevens, creditcardinformatie, pincode of andere persoonlijke informatie toe te sturen.

Ransomware

Ransomware is een specifiek computervirus dat probeert je geld te laten betalen om van het virus af te komen. Via ransomware kapen criminelen je computer of je hele IT-systeem, waardoor je niet meer bij documenten en foto’s kunt, of complete softwaresystemen niet meer kunt gebruiken. De criminelen beloven het virus te verwijderen en de blokkade op te heffen, als je een geldbedrag (vaak bitcoins) betaalt.

SQL-injectie

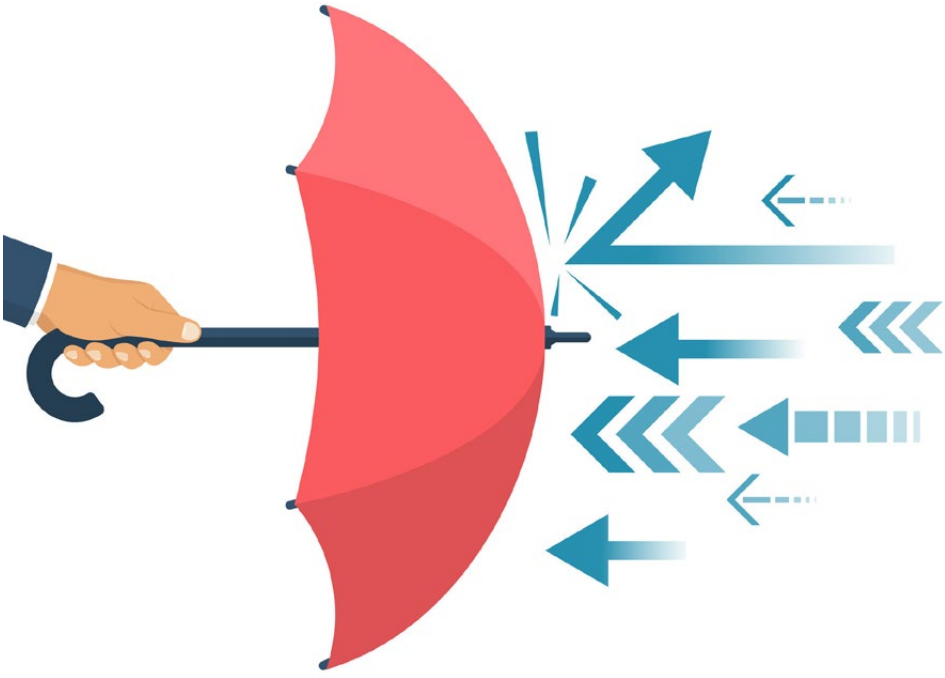
De term SQL-injectie staat voor Structured Query Language-injectie. Dit type cyberaanval is een veelgebruikte methode om een database ‘over te nemen’ en gegevens uit de database te stelen.

Botnet

Botnets zijn netwerken van computers die zonder medeweten van hun eigenaar besmet zijn met een virus of andere software en door derden worden misbruikt. Botnets worden gebruikt voor het versturen van spam en het uitvoeren van cyberaanvallen.

DDoS-aanvallen

Distributed denial-of-service (DDoS)-aanvallen hebben als doel een website of internetdienst onbruikbaar te maken door middel van overbelasting van de server. Vaak gaat het om websites van grote commerciële bedrijven, diensten van banken en creditcardmaatschappijen of e-maildiensten. De criminelen achter de aanvallen kunnen veel geld verdienen door hun diensten te verhuren of door bedrijven te chanteren. Particuliere websites zullen niet snel worden aangevallen, omdat er geen commercieel belang is.



2 Onze leefomgeving wordt volledig digitaal

Wat is een smart building of smart home en wat is de invloed van IoT?

De digitalisering van onze leefomgeving is niet meer te stoppen, maar ook niet meer weg te denken. Als we vanaf morgen geen computers, data en internet meer hebben, verdwijnt bijna al ons leefcomfort. Die invloed van digitalisering zal de komende jaren nog veel sterker worden, wanneer het Internet of Things (IoT), ofwel het Internet der dingen, groeit zoals onderzoekers dat nu voorspellen. IoT is het geheel aan apparaten dat met het internet verbonden is. Wereldwijd zijn dat er inmiddels bijna 30 miljard. We hebben het dan niet alleen over computers, laptops, tablets en smartphones, maar vooral ook over tv's, lampen, thermostaten, koelkasten, wasmachines, lantarenpalen, verkeerslichten, auto's en zelfs vuilnisbakken of (huis)dieren.

Al deze apparaten en objecten zijn met het internet verbonden middels wifi, bluetooth, vaste ethernet-verbindingen, mobiele verbindingen als 3G, 4G en 5G of speciale IoT-netwerken als LoRa. Door die internetverbinding kunnen ze communiceren met personen en met elkaar. De data die ze voortbrengen worden verzameld en geanalyseerd in 'the cloud', de verzameling van datacenters overal ter wereld waar we informatie bij elkaar brengen. Daardoor kunnen systemen, apparaten en voorwerpen soms zelfstandig besluiten nemen en bepalen welke inzet van hen nodig is, en die inzet automatisch in gang zetten. Dit gebeurt meer en meer zonder dat wij mensen er aan te pas hoeven komen.

Daarmee maakt IoT ons leven comfortabeler, beter, makkelijker en vaak ook veiliger. Apparaten en diensten worden bovendien efficiënter, waardoor het energiegebruik vermindert en de levensduur van apparaten langer wordt. Gebruikers hebben geen omkijken naar de inzet van de systemen, er is weinig of geen fysieke inspanning voor nodig.

Hoe werkt het IoT?
IoT-apparaten bevatten sensoren die gegevens verzamelen. Gegevens over bijvoorbeeld gebruik, slijtage, temperatuur, luchtvochtigheid en inval van daglicht. Een ingebouwde chip zorgt dat de apparaten de gegevens kunnen delen met personen en systemen. Door deze apparaten en componenten met sensoren en actoren die daarop weer kunnen reageren, in woningen en gebouwen te plaatsen, ontstaan smart homes en smart buildings. Als we die slimme leefomgevingen samenbrengen en koppelen, ontstaan smart cities.

Wat kun je er mee?

Het delen van informatie die de sensoren creëren of verzamelen, zorgt ervoor dat de apparaten of systemen waarin zij functioneren slim worden en biedt haar gebruikers inzicht. Op basis van de informatie die wij van de apparaten krijgen, kunnen we betere beslissingen nemen over de inzet ervan. Dat biedt gemak en comfort op kleine schaal, maar heeft op grotere schaal ook talloze andere mogelijkheden. Zo kunnen de IoT-toepassingen hele gebouwen of zelfs steden slim maken en kunnen we er, bij bedrijfsmatige toepassing van dergelijke omgevingen, commerciële beslissingen op baseren. We noemen hier vier belangrijkste toepassingen.

Smart building

Een smart building is een gebouw waarin allerlei slimme apparaten en systemen met elkaar samenwerken. Systemen voor bijvoorbeeld het binnenklimaat, de verlichting, audio-/videoapparatuur en de toegangscontrole. Ze kunnen via bussystemen of bekabeling binnen het gebouw met elkaar in verbinding staan. Maar vaker gebruiken we hiervoor een internetverbinding, zodat de systemen via het internetprotocol en servers met elkaar communiceren. Een smart building verzamelt ook data uit allerlei sensoren en slaat deze op in IT-systemen. Het gebouw leert zo van de gebruikers en wordt steeds slimmer. Daardoor kan het processen optimaliseren, fouten verminderen en de gebruikservaring verbeteren. Vanaf de parkeerplaats tot de ontvangstruimte en van de werkplek tot aan de vergaderzaal, denkt het gebouw met de gebruiker mee.

In een smart building is bijvoorbeeld zichtbaar welke ruimtes veel en weinig gebruikt zijn, zodat de schoonmaak daarop kan plannen en anticiperen. Ook kan in zo'n gebouw de luchtkwaliteit in drukke ruimtes op peil worden gehouden door meer ventilatie in te zetten als de CO2-waardes stijgen. Omdat bijna alle installaties worden gemonitord, functioneren ze beter en is gerichte inzet van onderhoud of vervanging mogelijk. Je kunt een werkplek ook op afstand reserveren en die laten voorverwarmen naar je eigen voorkeuren. Zijn er verschillende huurders? Dan verdeelt het slimme gebouw eenvoudig de energiekosten onder de diverse gebruikers.

Samengevat heeft een smart building een drietal voordelen. Namelijk:

- Het optimaliseren van gebouwprestaties, binnenklimaat en comfort op basis van de data die de slimme systemen voortbrengen;
- het verminderen van het energiegebruik;
- het verbeteren en vereenvoudigen van het gebouwbeheer.

Smart home

Een smart home functioneert feitelijk hetzelfde als een smart building, maar meestal op kleinere of beperkte schaal. Ook is de insteek hier vooral het gemak en de 'fun' van op afstand bedienbare apparaten en installaties. Zo kun je een woning laten voorverwarmen als je op weg naar huis bent. Maar de systemen bieden ook inzicht in wat er zich in de woning afspeelt en wat er aan energie wordt gebruikt. Uiteindelijk kan een slimme woning minder energie vragen en functioneert het beter en meer naar de persoonlijke wensen van de bewoners. Voorwaarde is dan wel dat de slimme systemen en apparaten in huis zijn verbonden via het internet en data met elkaar delen, zodat je er slimme koppelingen kunt maken.

De belangrijkste voordelen van een smart home zijn:

- Verhoogd comfort, persoonlijk instelbaar, ook op afstand.
- Efficiëntere inzet van systemen en apparaten;
- Betere veiligheid.

Smart cities

Een smart city (slimme stad) zet informatietechnologie en het IoT in om de stad te beheren en te besturen. Steden als Amsterdam, Utrecht en Eindhoven gebruiken data en algoritmes om de steden onder andere beter bereikbaar, schoner en veiliger te maken. Van sensoren in het wegdek die verkeersdrukte meten en daar de digitale bewegwijzering op afstemmen tot sensoren die de samenstelling van het rioolwater meten en vroegtijdig verontreiniging kunnen signaleren. Slimme lantaarnpalen zien het verkeer aankomen en gaan alvast feller branden. Vuilnisbakken, uitgerust met sensoren, geven door wanneer ze vol zitten en dus geleegd moeten worden.

Smart farming

Land- en tuinbouwbedrijven zetten het IoT in om zo efficiënt mogelijk de beste gewassen voort te brengen. Sensoren meten bijvoorbeeld hoe droog de grond is en bepalen – in combinatie met voorspellingen over regen – of en wanneer er beregend of gesproeid moet worden. De data van sensoren die meten hoe snel een gewas groeit, kunnen leidend zijn voor de inzet van kunstmest of kunstlicht. Melkrobots bepalen wanneer en hoe vaak een koe zich door een machine laat melken, zodat die niet met volle uier op de boer hoeft te wachten.

3 Hoe bescherm je jezelf tegen cybercrime?

Neem alle maatregelen die het cybercriminelen zo lastig mogelijk maakt.

Om te beginnen kun je jezelf, of een systeem dat op internet is aangesloten, nooit helemaal beschermen tegen cybercrime. Als hackers bij het Pentagon kunnen inbreken, dan komen ze ook in de systemen van jouw gebouw of woning. Wat je daarom wél kunt doen, is maatregelen nemen die het cybercriminelen zo lastig mogelijk maakt. Maatregelen waarmee je het risico op cybercriminaliteit zoveel mogelijk beperkt. Het Digital Trust Center geeft daarvoor vijf basisprincipes waarmee je - als je die naleeft - heel veel narigheid kunt voorkomen. Vandaar dat wij deze vijf principes hier kort samenvatten.

1 Kijk waar jouw systeem kwetsbaar is

Inventariseer in jouw bedrijf of in de woning welke onderdelen kwetsbaar zijn voor cyberdreigingen.

Een belangrijk actiepunt is het identificeren wat je in huis hebt en wat de kwetsbaarheden zijn. Breng bijvoorbeeld ook de technische afhankelijkheid van leveranciers in kaart. Een inventarisatie dwingt je om na te denken over wat je moet doen in het geval van een cyberincident. Dit helpt bij het opstellen van een noodplan en een bellijst.

Om de risico's te bepalen, kijk je naar:

- Beschikbaarheid - hoe erg is het dat een systeem het niet meer doet?
- Integriteit - hoe erg is het dat bepaalde gegevens niet juist zijn?
- Vertrouwelijkheid - hoe erg is het dat gegevens naar buiten lekken of verdwijnen?

Bepaal voor jezelf hoe groot de kans is dat een dreiging optreedt en wat de impact ervan is. Zo krijg je een beeld van de risico's voor jouw onderneming. Op de site van het Digital Trust Center is een stappenplan beschikbaar dat je kunt gebruiken voor een risicoanalyse.

2 Kies veilige instellingen

Controleer de instellingen van jouw apparatuur, software en netwerkverbindingen.

Leveranciers van apparatuur en software leveren deze vaak met standaard instellingen en wachtwoorden. Ook staan vaak standaard alle instellingen op 'aan'. Dit is erg handig voor het snel en eenvoudig installeren van nieuwe spullen of het krijgen van internettoegang. Maar als gebruiker in een woning of bedrijfspand ben je daardoor erg kwetsbaar voor cyberdreigingen, wanneer je deze instellingen vanaf het eerste gebruik niet wijzigt. Je zet dan de deur open voor onbevoegden.

Standaard instellingen en wachtwoorden maken dat iedereen de apparatuur, software en netwerkverbindingen direct vanaf internet kan benaderen. Het is secondewerk voor geautomatiseerde programma's om deze systemen online op te sporen. Cybercriminelen kunnen zo informatie in apparaten, software en netwerken, opvragen of veranderen. Ook is het apparaat, afhankelijk van het type, mogelijk op afstand te bedienen. Denk hierbij aan webcams en microfoons die criminelen, zonder dat je het weet, kunnen bedienen.

3 Voer updates uit

Check of jouw apparaten en software up-to-date zijn. Installeer direct beveiligingsupdates en schakel automatische updates in.

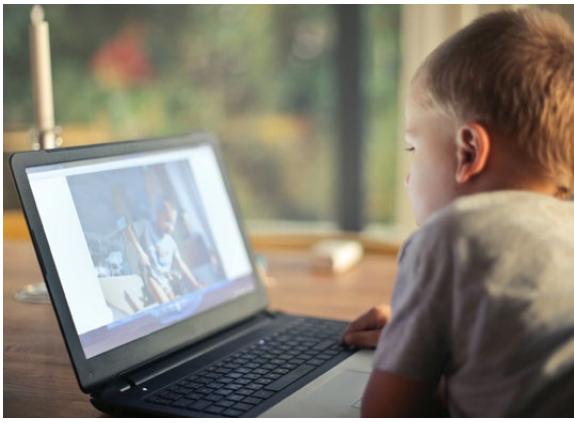
Producenten van apparaten, specifieke componenten en software zijn doorlopend bezig om hun producten door te ontwikkelen. Door middel van updates komen de nieuwste functionaliteiten bij de eindgebruikers terecht. Let bij de keuze van apparaten daarom ook op het 'updatebeleid' van de fabrikant. Wanneer je voor een apparaat kiest waarbij geen updatebeleid bekend is, haal je ook veiligheidsrisico's in huis. Zodra iemand kwetsbaarheden of een betere beveiliging ontdekt, bieden fabrikanten mét een updatebeleid vaak nieuwe functionaliteiten aan via updates. Installeer daarom in elk geval altijd direct de meest recente beveiligingsupdates zodat je zo goed als mogelijk beveiligd bent. Het is een feit dat software op elk apparaat veroudert als je geen updates uitvoert. Cybercriminelen weten dit ook. Zij zoeken vaak bewust naar kwetsbaarheden in verouderde software, om via die weg binnen te komen. Als je apparaten en software up-to-date zijn, loop je als bedrijf of vastgoedbezitter het minste kans op virussen en blijf je beschermd tegen de meest actuele cyberdreigingen en -risico's.

Tips om up-to-date te blijven

1. Negeer de automatische update notificaties van je apparaten of software niet. Zorg ervoor dat je de update zo snel mogelijk, maar tenminste binnen 24 uur installeert;
2. Abonneer je op alle notificatie-mogelijkheden van relevante leveranciers om zo tijdig notificaties van updates te ontvangen, of stel zelf notificaties in;
3. Geef de voorkeur, tijdens een selectieproces voor software of clouddiensten, aan leveranciers die een adequaat en effectief update-beleid en de daarbij behorende procedures hebben;
4. Maak heldere afspraken met leveranciers en zorg dat je weet welke patches relevant zijn voor je; leg vast wat je wel en niet doet in een logboek.

4 Beperk toegang

Definieer voor elke medewerker of gebruiker tot welke systemen en data hij of zij toegang nodig heeft om te kunnen werken. Zorg dat je toegangsrechten aanpast als iemand een nieuwe functie krijgt of bij de onderneming vertrekt.



Wil je de kans op ongelukken en misbruik zo klein mogelijk maken, dan moet je zorgen dat mensen binnen en buiten een onderneming alleen toegang hebben tot de systemen die passen bij hun werkzaamheden of de periode waarin zij dat werk moeten doen. Zorg dus voor een systeem van uitgebreide toegangsrechten zodat je exact weet wie waar toegang tot heeft.

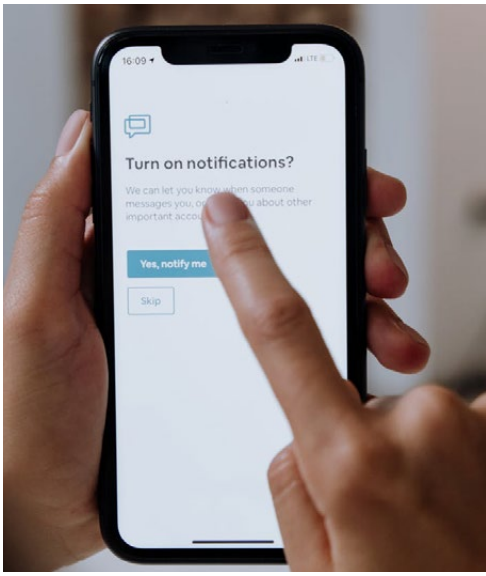
Hoe kun je dit goed organiseren?

1. Definieer per medewerker (of per bewoner) tot welke systemen en data diegene toegang moet hebben om zijn of haar werk te kunnen doen of om bepaalde functies te kunnen bedienen. Zo hoeven kinderen in een gezin bijvoorbeeld geen basisinstellingen te kunnen wijzigen.
2. Zorg er voor dat een medewerker, wanneer hij kan inloggen op de systemen, zich kan identificeren als die medewerker met bijbehorende toegangsrechten.
3. Gebruik veilige en sterke wachtwoorden en realiseer inloggen bij voorkeur door middel van twee-factor-authenticatie voor belangrijke systemen en data.
4. Beperk de fysieke toegang van medewerkers tot ruimtes waar systemen draaien (zoals servers) of apparaten (zoals externe harde schijven en USB-sticks) en documenten zijn opgeslagen.

5 Zorg dat systemen automatisch na een aantal minuten vergrendelen (locken), zodat deze niet toegankelijk zijn voor onbevoegden. Maak ook afspraken met medewerkers dat zij hun systeem zelf vergrendelen wanneer zij even van hun werkplek weglopen.
6 Zorg dat je de toegangsrechten aanpast als iemand een nieuwe functie krijgt of bij de onderneming vertrekt. Dit geldt ook als je bijvoorbeeld werkt met freelancers, tijdelijk personeel of externe toeleveranciers.

5 Voorkom virussen en andere malware

Stimuleer uw medewerkers tot veilig gedrag. Gebruik antivirussoftware en beperk de installatiemogelijkheden van software.

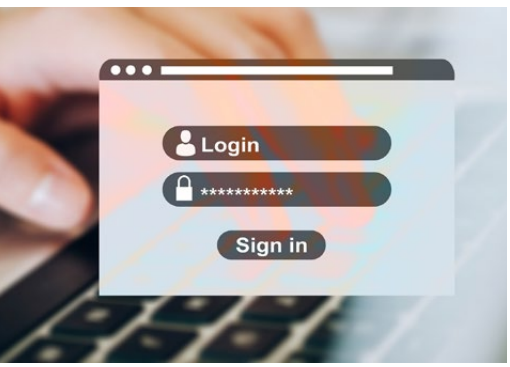


Virussen en malware kunnen echt enorme schades veroorzaken; ze kunnen systemen beschadigen, maar het wordt vaak nog erger als door dit soort bedreigingen data of bedrijfsgeheimen worden gestolen of ondernemers met ransomware worden afgeperst. Er zijn verschillende manieren waarop malware of virussen toegang krijgen tot computers, slimme systemen en netwerken in gebouwen of woningen of tot je smartphone. De zwakste schakel is bijna altijd een gebruiker; hij of zij kan een geïnfecteerde e-mail of bijlage openen, een foute website bezoeken of een besmet bestand via bijvoorbeeld een USB-stick openen. Binnen enkele seconden nadat de malware of het virus actief is, kan deze een systeem infecteren en zich als een olievlek naar andere apparaten en/of gebruikers verspreiden.

6 manieren om jezelf tegen malware te beschermen

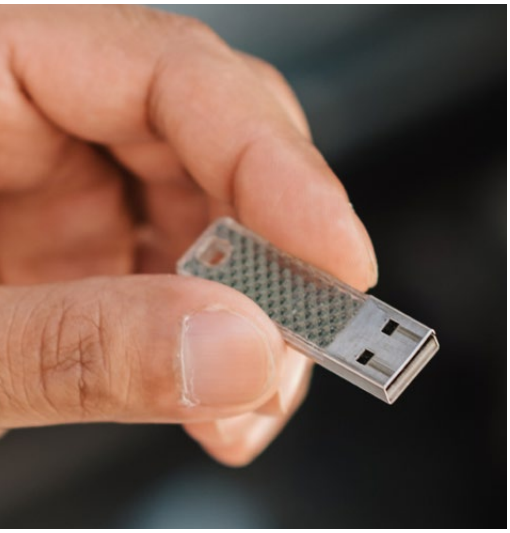
1 Stimuleer veilig gedrag van medewerkers. Cyberweerbaarheid staat of valt met het gedrag van medewerkers. Zijn jouw medewerkers of medebewoners voldoende bewust van de gevaren en de mogelijke gevolgen?
2 Gebruik een antivirusprogramma; een stuk software dat je apparaten bijna continu scant op de aanwezigheid van kwaadaardige software (malware). Een betaalde virusscanner wordt door de leverancier regelmatig bijgewerkt, zodat de software ook beschermt tegen de laatst bekende virussen.
3 Installeer apps bewust. Dus kies alleen apps uit een betrouwbare bron, zoals de downloadomgevingen van Android en Apple. Deze omgevingen controleren tot op zekere hoogte de betrouwbaarheid van apps. Binnen een bedrijf kun je beter alleen apps installeren die echt noodzakelijk zijn voor de bedrijfsvoering. In veel apps voor ‘vertier en vermaak’ ‘betaal’ je vaak met het weggeven van je persoonlijke informatie. Veel apps vragen bij installatie ook om toegang tot andere functies op je apparaat. Dat kan zijn de camera, locatiegegevens, je contactenlijst of zelfs je betaalmogelijkheden. Geef niet standaard alle toegang die gevraagd wordt maar bedenk wat echt noodzakelijk is. Daarmee beperk je het risico op lekken van informatie.
4 Beperk het aantal medewerkers met installatiemogelijkheden van software. Zo kun je beter voorkomen dat er besmette programma’s worden geïnstalleerd die mogelijk je bedrijfsnetwerk infecteren.
5 Steek niet zomaar een gevonden usb-stick of dvd in je apparaat. Grote kans dat hier malware op staat.

Samenvattend: gebruik je gezond verstand



- Wees voorzichtig wanneer je ongewenste of onbekende e-mails, berichten en telefoonoproepen ontvangt. Zeker in tijden van crisis gebruiken criminelen die situaties om je onder druk te zetten en om de gebruikelijke veiligheidsprocedures te omzeilen. De aanvallers weten dat het vaak gemakkelijker is om mensen te misleiden dan in te breken in complexe systemen. Onthoud dat banken en andere wettelijke entiteiten nooit je wachtwoord of inloggegevens zullen vragen.

- Beveilig je netwerk thuis of op het werk. Verander het standaard wachtwoord voor je wifi-netwerk en maak het sterker. Beperk het aantal



apparaten dat verbonden is aan je wifi-netwerk en laat alleen vertrouwde apparaten toe.

- Maak wachtwoorden sterk en voor elk apparaat uniek. Gebruik lange en complexe wachtwoorden met nummers, letters en speciale tekens.
- Bescherm je apparaten en systemen. Dit doe je door te zorgen dat alle systemen en programma's up-to-date zijn. Maar installeer ook antivirussoftware en update deze regelmatig. Plaats waar mogelijk fysieke en softwarematige barrières bij de toegang van jouw systeem naar het internet.
- Familie, bijvoorbeeld je kinderen, kunnen per ongeluk informatie wissen en aanpassen. Of erger, ze kunnen door hun surfgedrag, je computer, laptop of tablet per ongeluk infecteren. Dus laat je familie de apparaten die je voor je werk gebruikt, niet privé gebruiken.

4 Implementeer fysieke bescherming

De mogelijkheden om jouw digitale systemen te beschermen zijn verdeeld in vijf categorieën.

Digitale beveiliging, ofwel cyber security, wordt steeds belangrijker; misschien nog wel belangrijker dan een slot met politiekeurmerk of de beveiligingspoortjes bij de ingang van je gebouw. Een inbraak in onze digitale systemen en data kan in veel situaties verstrekkender gevolgen hebben, dan de diefstal van een portemonnee of schilderij uit de woonkamer of een laptop van een bureau. Helaas zijn veel slimme IT-systemen of IoT-netwerken in onze smart homes en smart buildings onnodig kwetsbaar voor hacks.

Die kwetsbaarheid ontstaat enerzijds doordat er fabrikanten zijn die nog onvoldoende investeren in de beveiliging bij productontwikkeling. Vaak gaat het dan om fabrikanten die goedkopere producten aanbieden. Anderzijds ook doordat afnemers beveiliging nog niet als criterium meenemen bij productkeuzes. Ook bij de installatie en integratie van netwerken laten gebruikers en installateurs soms steken vallen. De mogelijkheden die er wel degelijk zijn voor de beveiliging tegen een cyber-inbraak blijven nog te vaak onbenut. Wat zijn dan die mogelijkheden? We verdelen die hieronder in vijf categorieën.

Hardwaremaatregelen

Computers, sensoren en IoT-apparaten bevatten vaak gevoelige en essentiële informatie. Het is dus van groot belang om technieken te implementeren die bescherming bieden tegen aanvallen. Denk bijvoorbeeld aan XD-bit of NX-bit - beveiligingstechnologie in processors - voor computers. Omdat de beveiliging van een systeem zo sterk is als de zwakste schakel, moet dus echt elk verbonden apparaat in een slim gebouw aan strenge veiligheidseisen voldoen. Zo kun je voor hardware verplicht maken dat deze op geregelde momenten beveiligingsupdates ontvangt, controleert en installeert. Ook kun je eisen dat je kwetsbare ingangen als USB-poorten, webinterfaces en IP-poorten kunt afsluiten. Een andere maatregel is het toepassen van air walls die open wifi-verbindingen van bijvoorbeeld een slimme thermostaat beschermen.

Softwaremaatregelen

De software van programma's en systemen moet goed beveiligd zijn. Dat kan bijvoorbeeld door ze extra te laten scannen op malware, spyware en virussen. Firewalls beschermen software tegen hackers. In het eenvoudigste geval zorgt een firewall - een stuk software (of hardware) dat een verdedigingsmuur tussen jouw bedrijfsnetwerk en andere netwerken optrekt - voor een veilige verbinding. Binnen zo'n verbinding zal de firewall binnenkomend verkeer analyseren om uit te zoeken of het die software of data al dan niet in het netwerk moet toelaten. Zo zijn er dus verschillende soorten firewalls.
De twee meest voorkomende zijn:

- De standaard firewall op een computer. Deze is soms onderdeel van het besturingssysteem of kosteloos te downloaden en te gebruiken.
- Een firewall voor het hele netwerk. De implementatie en het beheer hiervan vergt specialistische kennis en brengt kosten met zich mee.

Daarnaast kun je maatregelen nemen om te voorkomen dat programma's of criminele organisaties systeeminformatie kunnen aanpassen. Ook is encryptie soms essentieel. Bestanden en datastromen moet je goed versleutelen om lekken te voorkomen.

Maatregelen omtrent gebruikers

Gebruikers vormen de meest kwetsbare groep als het gaat om cybercriminaliteit. Gebrek aan kennis van de risico's en van ICT, zorgen dat zij vaak de zwakste schakel zijn in slimme woningen en gebouwen. Zo stellen gebruikers vaak eenvoudige of standaard wachtwoorden in, die gemakkelijk te achterhalen zijn door hackers. Of ze verzaken om het wachtwoord vanuit de fabrieksinstellingen te veranderen. Kies altijd voor complexe wachtwoorden of zinnen en pas ze regelmatig aan. Daarnaast is het belangrijk dat consumenten en organisaties zich bewust worden van hun kwetsbaarheid en verantwoordelijkheid.

Managementmaatregelen

Vooral bij bedrijven en organisaties zijn risico-inventarisaties en cybermanagement van groot belang om kwetsbaarheden in kaart te brengen en op te lossen. Daaronder valt actief wachtwoordbeleid, server-beveiliging, toewijzing van toegang en bevoegdheden en het structureel updaten van programma's en beschermende software. Beleid maken op dit terrein en het naleven ervan wordt noodzaak voor het management.

Maatregelen bij ontwerp en installatie

Bij het ontwerpen van slimme systemen is een veilige IT-architectuur van groot belang. De gateway die besturingssystemen voor gebouwen verbindt met het internet, mag slechts beperkt toegankelijk zijn. Wel voor de installateur die op afstand problemen kan oplossen, maar niet voor kwaadwillende buitenstanders. Dat bereik je door het systeem niet via een standaardpoort van de router maar via een Virtual Private Network (VPN) te verbinden met het internet. Die VPN-verbinding moet meerdere lagen van beveiliging bevatten. Ook het programmeren van routers en wifi-accesspoints is van belang.

Een andere mogelijkheid is het afnemen van specifieke diensten die fabrikanten aanbieden om die veilige verbindingen zonder VPN te realiseren. In zo'n geval checkt een speciale server van een fabrikant of de verbinding veilig is, waarna deze via 'end-to-end-encryptie' toegang geeft tot een gebouw- of woningautomatiseringssysteem.

Wil je in een gebouw of woning ook een gastennetwerk aanbieden, richt daar dan een specifiek VLAN voor in, ofwel een virtual local area network. Die functioneert apart van het bedrijfsnetwerk, zodat gasten niet overal bij kunnen. Ook voor bepaalde slimme apparaten is het handig om een VLAN in te stellen. Zo kun je, door het gebruik van een firewall, voorkomen dat deze apparaten toegang hebben tot het hoofdnetwerk.

5 Rol voor de ontwerper en installateur

Wat is een router, een gateway en een VPN en hoe stel je ze in?

Om te zorgen dat een smart home of smart building op een veilige manier met het internet kan communiceren, moeten de ontwerper, installateur en systeem integrator adequate technische maatregelen nemen. Dit betekent dat de vakman moet weten hoe hij technisch gezien een veilige koppeling maakt met het internet, en welke hardware en software(instellingen) hij of zij daarvoor moet gebruiken. In dit hoofdstuk beschrijven we de meest belangrijke componenten voor een veilige verbinding. Zodra je deze componenten op een juiste manier voorschrijft, installeert en inregelt, is de beveiliging van het netwerk al in belangrijke mate zeker gesteld.

Het gebruik van een router

Een router zorgt dat je met meerdere apparaten tegelijk op het internet kunt, terwijl een modem zorgt dat de internetverbinding überhaupt werkt. Een modem en een router (eventueel draadloos) kunnen twee losse kastjes zijn, maar - zeker in de woning - zie je dat internetproviders vaak een modem met geïntegreerde router leveren. Deze noemen we modemrouter of wifi-modem.

Meestal is de modemrouter centraal in huis - in de meterkast of in het trappenhuis - geplaatst. In (grote) gebouwen zijn router en modem in de meeste gevallen losse apparaten. Achter een router kun je nog één of meerdere switches installeren wanneer je de internetbekabeling over meerdere werkplekken wilt verdelen. De gewone switch is echter niet meer dan een ‘verdeler’ die het inkomende internet verdeelt over meerdere uitgangen. Maar er bestaan ook smart switches, die zijn vooral noodzakelijk bij het gebruik van VLAN’s omdat ze het verkeer tussen verschillende netwerkpoorten kunnen blokkeren. Een ander stuk hardware dat je in veel gebouwen tegenkomt, zijn versterkers of repeaters. Vaak zijn deze verbonden aan een internetkabel en zenden het wifi-signaal uit, omdat de router die het wifi-signaal uitzendt te ver weg staat.

Het gebruik van een gateway

Een gateway is in het algemeen een netwerkapparaat dat als toegangspunt fungeert van het ene netwerk naar een ander netwerk (of andere netwerken). Het apparaat vormt de fysieke koppeling of link tussen twee systemen die je met elkaar (of met het internet) wil verbinden. In woning- en gebouwautomatisering fungeert de gateway in veel gevallen ook als portaal en communicatiemiddel tussen protocollen. Zo zorgt dit apparaat ervoor dat twee systemen of netwerken met verschillende protocollen gegevens kunnen delen.

De gateway stelt de gebruikers van automatiseringssystemen in staat om de verschillende data voor bijvoorbeeld commando’s of monitoring onderling uit te wisselen. Je kunt daarbij denken aan uitwisseling van data tussen twee technische systemen met ieder hun eigen protocol, waarbij zo’n systeem natuurlijk ook het internet kan zijn. Kortom, zonder gateway kunnen de meeste automatiseringssystemen niet van het internet gebruik maken.

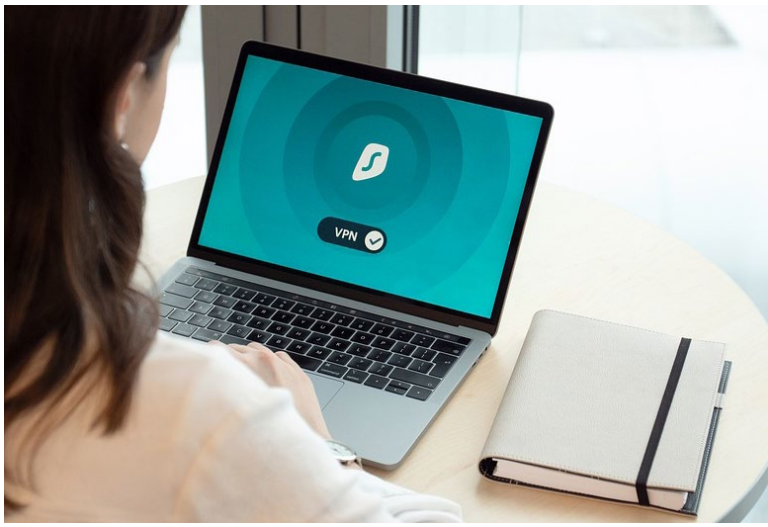
Je kunt de gateway voor onder meer de volgende functies gebruiken:

- Als methode om communicatie via verschillende media tussen verschillende netwerken te realiseren, omdat elk netwerk andere protocollen en kenmerken heeft.
- Als een interface tussen lokale en wide area protocollen zoals TCP/IP op het internet.
- Als belangrijk mechanisme voor elke vorm van telefonische communicatie die een verbinding vormt tussen het telefoonnetwerk en het internet.

Gateway versus router

Vaak wordt er een vergelijking gemaakt tussen een router en een gateway. Toch zijn deze apparaten niet hetzelfde en hebben ook niet dezelfde functie. Het klopt dat je de gateway en de router beiden kunt gebruiken om het netwerkverkeer tussen twee of meer afzonderlijke netwerken te regelen. Gateways zijn echter in staat om het verkeer tussen twee verschillende netwerken (KNX en internet of BACnet en internet) te regelen, terwijl routers het verkeer tussen vergelijkbare netwerken (internet) regelen. Gateways kun je ook gebruiken om het netwerkverkeer te verminderen of te reguleren, en dat kan een router niet. Ook kan een gateway, in tegenstelling tot een router, de communicatie in en tussen verschillende omgevingen of netwerken tot stand brengen. Terwijl je een router weer kunt gebruiken om het verkeer op bedrijfsnetwerken te segmenteren.

Het gebruik van een VPN



VPN is de afkorting van Virtual Private Network. Via een VPN-verbinding krijgt de gebruiker versleutelde en omgeleide (anonieme) toegang tot een netwerk. Daardoor is de verbinding met het internet, en dus ook je online gegevens, beveiligd. Hackers, maar ook overheden, internetproviders of je werkgever, kunnen het internetverkeer niet meer volgen én niet achterhalen waar je je bevindt. Daarmee is het een must bij het tegengaan van digitale inbraken en aanvallen.

VPN is als een veilige, geheime tunnel onder de openbare, digitale snelweg. Door die tunnel verloopt alle communicatie met het internet. Elk verzoek dat je stuurt en elk ‘antwoord’ dat je krijgt, wordt met een slot erop (encryptie) door de veilige tunnel geschoten. De VPN-software op je computer of smartphone pakt elk datapakketje voor je in voordat het de tunnel in gaat en pakt het datapakketje uit wanneer er iets terugkomt. Onderweg zijn die datapakketjes niet te onderscheppen of open te breken. De communicatie vindt niet rechtstreeks plaats tussen jou en bijvoorbeeld de website die je bezoekt, maar middels de VPN-server.

VPN is er in verschillende ‘smaken’. Om optimaal gebruik te maken van een VPN-verbinding, moet je een keuze maken voor het VPN-protocol dat voor jouw toepassing het meest geschikt is. Zodra je die keuze hebt gemaakt, installeer je de benodigde technologie op jouw systeem en dat van de klant waarmee je contact wil maken.

Beveiligde cloudservices

Naast een keuze voor een VPN kun je ook kiezen voor een veilige verbinding die diverse hardware-leveranciers aanbieden. In dat geval bieden zij, met hulp van hun hardware, een verbinding aan die wordt gecontroleerd door een beveiligde server van die leverancier. Zodra de beveiliging in orde is, verleent die server toegang tot een bepaald automatiseringssysteem. Die verbinding vindt dan plaats via ‘end-to-end-encryptie’. Voorwaarde is wel dat jij die leverancier vertrouwt. Ook blijft deze verbinding in stand zolang de leverancier deze ondersteunt of überhaupt bestaat.

6 Welke gevaren liggen er op de loer; de praktijk

Met de opkomst van slimme gebouwen hebben cybercriminelen een nieuwe prooi in hun vizier.

De transitie naar een wereld die verbonden is via het internet, brengt ongekende mogelijkheden, maar ook gevaren met zich mee. Het aantal slimme apparaten groeit razendsnel. De informatie die ze naar de cloud sturen, is in principe kwetsbaar voor toegang en zelfs aanvallen van buitenaf. Hoe meer apparaten er verbonden zijn via het internet, hoe moeilijker het wordt om de grote hoeveelheid data die ze voortbrengen te beveiligen. Daarmee neemt ook het gevaar van datalekken, hacks en cracks toe.

Systemen kunnen worden gehackt om data te stelen, om ze te manipuleren of om ze ontoegankelijk te maken. Een virus dat jouw data wist of ransomware dat jouw data ontoegankelijk maakt (tot je betaalt) zijn bekende voorbeelden van cybercriminaliteit. Met de opkomst van slimme gebouwen hebben cybercriminelen een nieuwe prooi in hun vizier. Uit een rapport van RiskBased Security blijkt dat in 2019 zo'n 8,5 miljard gegevensrecords openbaar werden als gevolg van datalekken. Dat is twee keer zo veel als in dezelfde periode in 2018. En dat die datalekken of datadiefstallen in veel gevallen op zeer eenvoudige of naïeve wijze tot stand kunnen komen, blijkt uit een aantal bekende voorbeelden.

Ongewenste acties veroorzaken

Omdat door het internet alles met elkaar verbonden is en apparatuur op afstand kan worden bestuurd, kunnen kwaadwillende buitenstaanders via bijvoorbeeld slecht beveiligde IoT-apparaten complete smart home of smart building-systemen overnemen en besturen. Ze kunnen instellingen voor de besturing veranderen zodat de systemen tot ongewenste acties overgaan. Bekende voorbeelden uit voorgaande jaren van deze manier van 'inbraken' zijn Stuxnet, waar buitenstaanders overgingen tot aanpassingen van de centrifugesnelheid in een fabriek. Maar ook een energiecentrale in Oekraïne die werd platgelegd door cybercriminelen.

Devil's Ivy richt veel schade toe

Enorm veel IoT-apparaten blijken slecht of helemaal niet beveiligd te zijn. In 2017 werd een kwetsbaarheid ontdekt in een groot aantal IoT-apparaten; een zaak die bekend werd onder de naam Devil's Ivy. De werkwijze van een aanval op deze kwetsbaarheid is simpel en doeltreffend. De aanvaller benadert een kwetsbaar apparaat, zoals een ip-camera of een slim lichtarmatuur. Door het terugzetten van de fabrieksinstellingen neemt de aanvaller het apparaat over.

Gebruikmakend van het apparaat, breekt de aanvaller vervolgens in op de router, of hij wacht tot er iemand inlogt op de router waarna hij door middel van sniffing het wachtwoord achterhaalt. Door de router over te nemen kan de aanvaller ook de goed beveiligde IoT-apparaten en andere systemen benaderen op het netwerk.

Mirai-malware infecteert 100.000 IoT-apparaten

DDoS staat voor Distributed Denial of Service. Met een DDoS aanval maken heel veel computers – vaak vanaf verschillende locaties ter wereld – verbinding met één server. In 2016 zijn aanvallers erin geslaagd om een succesvolle DDoS-aanval te plegen op het internetbedrijf Dyn. Mirai-malware infecteerde meer dan 100.000 IoT-apparaten met een default wachtwoord. Veel bedrijven waren door die aanval urenlang niet bereikbaar. Twitter, CNN, NetFlix en Reddit waren de bedrijven die uiteindelijk het meeste last hadden van deze grootschalige aanval, die voorkomen had kunnen worden door het veranderen van het default wachtwoord op de IoT-apparaten.

Controle over slimme apparaten overgenomen

In 2019 vond een opmerkelijk datalek plaats bij Orvibo, een producent van IoT- en smart home-apparatuur. Door dit lek lagen twee miljard records van apparatuur bij een miljoen verschillende klanten op straat, inclusief wachtwoorden, mailadressen, geolocatie-data, ip-adressen en namen. Met die gegevens was het mogelijk om accounts te kapen en de controle over te nemen van de ‘slimme’ apparaten die via Orvibo werden geleverd en nog worden beheerd.

Betalen of zweten

Begin 2020 slaagden ethische hackers er in om de slimme thermostaten van een aantal gebouwen in Amerika over te nemen. Dat deden ze door een virus te installeren op de SD-kaart, waarna ze door middel van ransomware de gebouweigenaar voor een keuze konden stellen: 500 dollar betalen of anders ging de thermostaat omhoog naar de maximale stand van 37 graden Celsius.

7 Veilige gebouwautomatisering met KNX Secure

Een KNX-systeem dat via een openstaande poort 3671 op de router benaderbaar is, is altijd onveilig.

‘Honderden slimme gebouwen te kraken’ kopte de NOS op 21 februari 2019. Een ethische hacker van beveiligingsbedrijf Computest vond in Nederland ruim 1300 gebouwen met slecht of niet beveiligde slimme systemen en apparaten. In hun test keken zij naar gebouwen die de KNX-standaard gebruiken en die via een openstaande poort 3671 op de modem(-router) met internet verbonden zijn. Maar voor hetzelfde geld hadden zij naar elk ander domotica- of woningautomatiseringssysteem met internetaansluiting kunnen kijken. Want dáár zit het probleem. Zodra een slimme woning een koppeling met internet heeft, is ze in principe onveilig, tenzij die verbinding met internet beveiligd is. Een beveiliging die verder gaat dan een wachtwoord.

Voor de ethische hackers van Computest ging het er om te laten zien dat die beveiliging er vaak niet is. En als consument of eigenaar van een woning of gebouw kun je dat meestal zelf niet beoordelen. De vakman die de installatie installeert, programmeert en beheert, moet die beveiliging aanbrengen. En op dit moment is die beveiliging op redelijk grote schaal, door een gebrek aan kennis en te weinig bewustzijn, minder goed geregeld. Daardoor kunnen kwaadwillenden, zo melden de ethische hackers, de slimme systemen op afstand inzien en soms zelfs bedienen. In het artikel wekte de ethische hacker de indruk dat slimme systemen, die aan het internet gekoppeld zijn, ook gemakkelijk over zijn te nemen nadat je via internet toegang hebt gekregen. gemakkelijk over te nemen zijn. Maar is dat wel zo?

Check de veiligheid

Het antwoord op bovenstaande vraag is niet eenduidig. Zodra je jouw gebouw- of woningautomatisering via een onveilige verbinding aan internet koppelt om deze op die manier overal vandaan en met allerlei mobiele devices te kunnen besturen, zijn de slimme systemen inderdaad eenvoudig op afstand te benaderen. De veiligheid van die systemen hangt in dat geval af van het wel of niet beveiligen van de internetverbinding waarmee de domotica of gebouwautomatisering is gekoppeld. Het feit dat de router met een wachtwoord is beveiligd, betekent niet automatisch dat jouw domoticasysteem of woningautomatisering beveiligd is.

Een vakbekwame installateur weet dat hij ten minste een Virtual Private Netwerk (VPN) of een andersoortig ‘dedicated netwerk of cloudserver’ voor de woning- en gebouwautomatisering zal moeten realiseren.

Nieuwe maatregelen

Maar er komen andere mogelijkheden op de markt, met name voor de meer geavanceerde gebouwautomatiseringssystemen. Woningen en gebouwen met intelligente automatisering zijn namelijk goed te beveiligen tegen digitale inbraken. Fabrikanten die lid zijn van KNX Nederland en van de Brancheorganisatie Gebouw Automatisering kunnen in toenemende mate een compleet pakket aanbieden van veilige oplossingen voor woning- en gebouwautomatisering. Zo werkt de internationale KNX Association al jaren samen met tientallen universiteiten om de beveiliging van de systemen te verbeteren. Deze verbeteringen zijn grofweg in te delen in twee categorieën: de beveiliging van het protocol KNX en de beveiliging van de KNX-producten. Tot slot werkt KNX bij vakmensen die met KNX werken ook aan het vergroten van het bewustzijn van het belang van een veilige koppeling van KNX met internet.

Starten met bewustwording

Op het gebied van bewustwording doet KNX Nederland er samen met brancheorganisaties en opleidingsinstellingen alles aan om zoveel mogelijk kennisdocumenten beschikbaar te stellen voor professionals die met KNX werken. Voorbeelden hiervan zijn de KNX-security checklist en de KNX-security positioning paper. Beide documenten zijn te downloaden via de online community Smart Inside. In Nederland organiseerde KNX al diverse netwerkbijeenkomsten en workshops over KNX, IP en beveiliging.

Beveiligingsconcept KNX Secure

Om ook het gebruik van systemen en componenten met het KNX-protocol via het internet goed te beveiligen, ontwikkelde de KNX Association het beveiligingsconcept KNX Secure. Deze technologie beveiligt zowel de koppeling van het automatiseringssysteem met internet als het dataverkeer tussen specifieke componenten binnen een KNX-systeem. De internationale standaardiseringscomités stelden in 2017 al vast dat KNX Secure voldoet aan de hoogste veiligheidseisen op het gebied van cyber security - de encryptiestandaard AES128 CCM - waarna technologie is gestandaardiseerd volgens EN 50090-4-3 en ISO 18033-3. In de praktijk bestaat de beveiliging uit een dubbel beschermingsconcept dat is op te delen in twee mechanismen:

- KNX IP Secure,
- KNX Data Secure.

KNX IP Secure zorgt dat de communicatie tussen de KNX-installatie en het internet is beveiligd. De specifieke hardwarecomponent die de koppeling tussen een KNX-systeem in het huis of gebouw met het internet verzorgt, zorgt dat de toegang tot het systeem is versleuteld. Alleen als je de ‘digitale sleutel’ hebt, kun je op het systeem binnenkomen. KNX Data Secure codeert ook de datagegevens op de buslijn. Het gaat dan om de informatie die tussen specifieke componenten of systeemonderdelen via het bussysteem worden verstuurd. Op die manier kan de informatie die tussen die beveiligde componenten loopt, alleen worden gelezen door componenten die over de intelligentie beschikken om die gegevens te decoderen.

Korte technische uitleg

KNX Data Secure zorgt dus dat, ongeacht het gekozen KNX-medium (twisted pair, IP, draadloos), berichten die door KNX-componenten worden verzonden, kunnen worden geverifieerd en/of gecodeerd. Om de technologie nog veiliger te maken, zijn bovenop KNX Data Secure de KNX IP Secure-mechanismen gedefinieerd. Daarmee is extra veiligheid ingebouwd in het geval dat de communicatie via Data Secure niet beveiligd zou zijn en de netwerken wel met IP zijn verbonden.
KNX Data Secure-componenten gebruiken een langer KNX-telegramformaat bij het verzenden van de geauthentiseerde en gecodeerde gegevens. Dit heeft geen effect op de reactiesnelheid van componenten

op de KNX-bus. Met KNX IP Secure wordt een beveiligde verbinding (tunneling of componentbeheer) tot stand gebracht. Op deze manier zorgt KNX IP-tunneling of routing ervoor dat telegrammen via IP niet kunnen worden opgepikt of gemanipuleerd. De KNX IP Secure-mechanismen zorgen ervoor dat er een ‘veiligheidslaag’ wordt toegevoegd rond het volledige KNXnet/IP- dataverkeer.

Veilige hardware kiezen

Met KNX IP Secure beveilig je dus de toegang tot het systeem. En met KNX Data Secure kun je specifiek berichten of informatie op het bussyteem ook nog eens gericht coderen en daarmee beveiligen. KNX Secure is daarmee een concept waarmee de systeem integrator elke gebruiker van een KNX-systeem in steeds verdergaande mate een gegarandeerd veilige woning- of gebouwautomatisering kan bieden. De componenten voor het KNX Secure-concept verschijnen sinds 2018 op de markt. Nog niet alle componenten en beveiligde routers zijn volledig beschikbaar. De fabrikanten hebben enige tijd nodig om alle cruciale gateways, routers en andere componenten met de KNX Secure-technologie uit te rusten. Op de online community Smart Inside staat inmiddels een productbrochure met componenten die beschikbaar zijn of zeer binnenkort beschikbaar komen. Ook op de website van KNX.org worden nieuwe componenten continu aangekondigd.

8 Over KNX

KNX is de enige wereldwijd erkende standaard voor woning- en gebouwautomatisering. KNX is een communicatieprotocol dat kan worden gebruikt om installaties en apparaten te automatiseren en te koppelen. Het gaat daarbij om uiteenlopende installaties; van verlichting tot verwarming, van beveiliging tot ventilatie, maar ook audio en video, slimme energiemeters en zelfs witgoed, zoals wasmachines of wasdrogers.

KNX zit ingebouwd in bijna 10.000 componenten en systemen van fabrikanten (wereldwijd al 500 bedrijven) die zich bij de KNX Association hebben aangesloten. Omdat al die producten hetzelfde, uniform gecertificeerde protocol gebruiken, kunnen al deze componenten onderling worden gekoppeld, ongeacht wie het product fabriceert. Dit bezorgt opdrachtgevers veel meer keuzevrijheid en een toekomstvast automatiseringssysteem. KNX is dus decentrale intelligentie die in elk KNX-gecertificeerd component aanwezig is. Daardoor kan elke installateur en system integrator die met KNX kan werken, de componenten en systemen tot één geheel smeden.

Wil je meer weten over de mogelijkheden van het protocol en de automatisering van technische installaties met KNX? Download dan het digitale KNX Adviseurshandboek op www.smartinside.nl -> Documenten. Of vraag een gratis gedrukt exemplaar aan via een mail naar info@knx.nl.

KNX Nederland

KNX Nederland is een vereniging die bestaat uit fabrikanten, leveranciers, importeurs en groothandelaren van KNX-producten en/of -systemen of producten die compatibel zijn met het communicatieprotocol KNX. Het doel van KNX Nederland is om de toepassing van KNX als protocol en systeem in de markt te bevorderen. Dit doet de vereniging door elk jaar diverse marketing- en communicatie-acties uit te voeren.
Meer informatie op www.knx.nl.

Alle fabrikanten en leveranciers van producten en/of systemen die op KNX zijn geënt, kunnen lid worden van KNX Nederland. Dit kan als KNX-fabrikant, als vertegenwoordiger van KNX-fabrikanten of als leverancier van producten die met KNX-gecertificeerde producten kunnen worden geïntegreerd. Alle leden moeten de doelstellingen van de vereniging onderschrijven. Huidige KNX-fabrikanten die lid zijn van KNX Nederland:

- ABB
- B.E.G. Luxomat
- Gira
- Hager
- Hateha/JUNG
- Mean Well
- Siemens
- Theben Nederland
- Xxter

KNX GroothandelsPartners zijn groothandelaren die KNX-producten leveren en naar de markt het signaal afgeven dat zij bijdragen aan de markt voor installaties die via KNX te automatiseren zijn. De huidige KNX

GroothandelsPartners zijn:

- Oosterberg
- Solar Nederland
- Technische Unie

KNX Associates zijn bedrijven die producten of systemen hebben die met KNX kunnen samenwerken. De Associates zijn ook kennisinstellingen of organisaties die een informerende en/of adviserende rol binnen de markt vervullen en zo KNX Nederland ondersteunen bij de groei van woning- en gebouwautomatisering in het algemeen en KNX in het bijzonder. De huidige KNX Associates zijn:

- Alphatronics BV
- Brancheorganisatie Gebouw Automatisering
- Instaver Systems
- Leertouwer
- Osec
- Smart Homes

KNX Trainingscentra

Elke installateur of system integrator die op vakkundige wijze een KNX-installatie wil realiseren, doet er goed aan een gecertificeerde KNX-opleiding te volgen. Deze opleidingen worden gegeven door internationaal gecertificeerde opleidingscentra. In Nederland zijn op dit moment zeven gecertificeerde KNX-opleidingscentra die ook het gecertificeerde KNX-examen afnemen. Elke vakman die voor het examen slaagt, krijgt de status KNX Partner en mag zich vervolgens als KNX Professional in de markt onderscheiden. Dit zijn de Nederlandse KNX Trainingscentra:

- ABB, Ede
- Domotica-opleidingen.nl, Raamsdonksveer
- Hager, Den Bosch
- Hestia Opleidingen B.V., Laren
- InstaVer Systems B.V., Nieuw-Vennep
- Oosterberg, Ede
- Stichting Kenteq, Hilversum
- xxter, Amsterdam

KNX Professionals

KNX Professionals zijn installateurs en systeem integratoren die met KNX werken en zich als duidelijk erkende vakman willen onderscheiden. Dit doen zij door lid te worden van de community Smart Inside. Deze community is opgericht door KNX Nederland om vakmensen die met KNX werken een podium te geven en hen in contact te brengen met alle andere professionals in de wereld van woning- en gebouwautomatisering.

Meer informatie vind je op https://smartinside.nl

smartinside
Building connections

9 Aandachtspunten bij cyber security op een rij

Introductie - waar gaat het om en waar liggen de risico's

- **Cyber security gaat over de beveiliging van geautomatiseerde systemen en digitale gegevens.**
- **Slimme systemen en apparaten die met internet zijn verbonden, zijn kwetsbaar; cyber criminelen misbruiken de koppeling met internet als deze niet goed is beveiligd.**
- **Er zijn drie soorten cyberdreigingen:**
  - Cybercriminaliteit; criminelen die systemen aanvallen voor financieel gewin via diefstal of afpersing of het veroorzaken van storingen die voor financiële schade zorgen.
  - Cyberaanval; gericht op het misbruiken van informatie via het aangevallen systeem of het lamleggen van bepaalde systemen.
  - Cyberterrorisme; terroristen die via een aanval op systemen proberen angst en paniek te verspreiden onder een grote groep mensen.
- **Veelgebruikte methoden van cyber criminelen:**
  - Virus; een programma dat de werking van de geïnfecteerde computer beïnvloedt, zoals het aantasten van programma's of het wissen van de harde schijf.
  - Malware; kwaadaardige software om de werking van (computer)systemen te verstoren.
  - Phishing; criminelen vragen in officieel lijkende communicatie naar belangrijke persoonlijke gegevens. Deze informatie wordt vervolgens gebruikt om geld afhandig te maken.
  - Ransomware; een specifiek virus waarmee een computer of IT-systeem onbruikbaar wordt gemaakt ('gegijzeld'). Criminelen vragen een geldbedrag om de blokkade op te heffen.
  - SQL-injectie; Dit type cyberaanval is een veelgebruikte methode om een database 'over te nemen' en gegevens te stelen.
  - Botnet; netwerken van computers die zonder medeweten van hun eigenaar besmet zijn. Botnets gebruikt men voor het versturen van spam en het uitvoeren van cyberaanvallen.
  - DDoS-aanval; aanvallen met als doel een website of internetdienst onbruikbaar te maken door middel van overbelasting van de server.
- **Opkomst van het Internet of Things (IoT), het geheel van apparaten dat met internet is verbonden, is vaak matig tot slecht beveiligd.**
- **Sensoren in slimme automatiseringssystemen verzamelen gegevens, die via internet in 'the cloud' samen komen. Op basis van deze data kunnen systemen en apparaten efficiënter functioneren en zijn ze op afstand aan te sturen.**
- **Door IoT en sensoren op grote schaal toe te passen, kunnen we complete gebouwen, steden en land- en tuinbouwbedrijven 'smart' maken.**

Maatregelen - hoe voorkom je gevaar en wat kun je doen

- **Inventariseer waar je systeem kwetsbaar is.**
- **Kies veilige instellingen en wachtwoorden.**
- **Voer altijd de laatste updates uit.**
- **Beperk toegang tot het systeem.**
- **Zorg ervoor dat hardwaresystemen goed beveiligd zijn.**
- **Selecteer hardware waarvan de toegang tot internet 100% veilig is.**
- **Wees alert op virussen en andere malware in je systemen.**
- **Gebruik beveiligingssoftware zoals firewalls en antivirusprogramma's.**
- **Gebruik je gezond verstand bij alles wat je (online) doet.**
- **Maak elke gebruiker bewust van zijn gedrag en de veiligheidsrisico's.**
- **Zorg binnen bedrijven voor een actief beleid voor 'cybermanagement'.**
- **Kies voor slimme systemen met een veilige IT-architectuur.**
- **Vraag je leverancier hoe zijn systeem of component veilig met internet koppelt.**

10 Bronnen en verantwoording

De inhoud van deze whitepaper is tot stand gekomen op basis van vele bronnen; geschreven bronnen, presentaties en personen die voor deze teksten zijn geïnterviewd. Belangrijke bronnen zijn:

Digital Trust Center	www.digitaltrustcenter.nl
National Cyber Security Centrum	www.ncsc.nl
Consumentenbond	www.consumentenbond.nl
Speedcheck	www.speedcheck.org
VPN Gids	www.vpngids.nl
Security Management	www.securitymanagement.nl

Speciale dank aan Martin van Ling (Hestia Domotica) en Freddy van Geel (xxter).

Redactie en vormgeving, i.o.v. KNX Nederland: Stijlmeesters (www.stijlmeesters.nl)