KPMG

Smart Building Security

Beschermen van slimme kantoren en huizen tegen relevante cybersecurityrisico's

Pak de risico's voor slimme gebouwen aan die er echt toe doen

Dat cybersecurity belangrijk is voor elke organisatie, dat behoeft eigenlijk geen nadere toelichting. Vrijwel dagelijks bewijzen incidenten dat de risico's groot zijn en dat zowel individuele hackers als professioneel georganiseerde cybercriminelen zich roeren. Met de opkomst van de slimme gebouwen is er een nieuwe prooi op de markt voor deze aanvallers. Cybersecurity is een complex thema, in deze flyer geven we de handvatten hoe cybersecurity toegepast kan worden voor uw smart building-oplossing. Eerst zullen we de meest gemaakte denkfouten benoemen. Om daarna de aandachtspunten voor smart building security voor u op een rij te zetten.

Vijf veel gemaakte denkfouten in cyber security

Denkfout 1:	We moeten gaan voor 100% beveiliging
Werkelijkheid:	100% zekerheid is onhaalbaar en ongewenst
Denkfout 2:	Als we investeren in best-of-class tools, dan zijn we veilig
Werkelijkheid:	Cybersecurity gaat minder om technologie dan u denkt
Denkfout 3:	Onze wapens moeten beter zijn dan die van de hackers
Werkelijkheid:	Het beveiligingsbeleid wordt primair door u bepaald, niet door de aanvallers
Denkfout 4:	We moeten streng controleren of de cybersecurity procedures worden nageleefd"
Werkelijkheid:	Het vermogen om te leren is belangrijker dan het vermogen om te controleren
Denkfout 5:	We moeten de beste professionals aantrekken om ons te wapenen tegen cybercrime"
Werkelijkheid:	Cybersecurity is geen afdeling maar een houding

Drie aandachtsgebieden voor effectieve maatregelen

Preventie:

Preventie begint met bewustzijn en organisatie. Het gaat naast technische maatregelen onder andere om het beleggen van de verantwoordelijkheid voor cybersecurity in de organisatie en om bewustwordingstrainingen voor alle medewerkers.

Detectie:

Een organisatie kan door het monitoren van kritieke en onverwachte gebeurtenissen binnen de organisatie en extern beschikbare informatie over cyberdreigingen de technologische detectiemaatregelen versterken. Monitoring en data analyse vormen samen een uitstekend instrument om vreemde patronen in het gegevensverkeer op het spoor te komen, te signaleren waar de aanvallen zich concentreren en de systeemprestaties te observeren.

Respons:

Bij respons gaat het om het in werking stellen van een plan zodra zich een aanval voordoet. Bij een aanval moet de organisatie adequaat kunnen reageren. Bij de ontwikkeling van een respons- en herstelplan doet een organisatie er goed aan (informatie)beveiliging te zien als een continu proces en niet als eenmalige oplossing.

Smart Building Security

Beveiligen van Smart Buildings

Een Smart Building is toekomstbestendig en kan met vertrouwen worden gebruikt of bewoond

Aanbieder van slimme gebouwen

Innovaties in de informatie technologie en domotica worden op grote schaal toegepast in de vastgoed- end bouwsector. Als bouwonderneming of vastgoedaanbieder onderscheidt u zich door steeds 'slimmere' gebouwen aan te bieden. Echter komt hier veel bij kijken op het gebied van technologie, bedrijfsvoering, wet- en regelgeving, privacy en informatiebeveiliging.

De mogelijk toepassingen van smart buildings zijn talrijk; van het verhogen van het gebruikscomfort door het automatiseren van (dagelijkse) handelingen, tot het bieden van inzichten in energieverbruik, tot het ondersteunen van zorgbehoevenden in hun specifieke woonbehoeften. Met de opkomst van stemassistenten zal de aansturing van de systemen nog dichter in het dagelijks leven komen.

Om deze toepassingen mogelijk te maken, worden de systemen in het gebouw verbonden aan het internet. Daarmee zijn zij in potentie ook benaderbaar door kwaadwillende van buitenaf. Wanneer de beveiliging van de systemen niet voldoende bescherming biedt, kan dit leiden tot ernstige gevolgen voor de beveiliging van de woning (slimme sloten en alarmen), de privacy van de gebruikers/bewoners, alsook financiële en reputatieschade voor u als bouwer of aanbieder van de slimme gebouwen.

KPMG Cyber ondersteunt Smart Building Security door:

- het helpen ontwerpen en implementeren van veilige domotica-systemen;
- het inzichtelijk maken van beveiligings- en privacyrisico's voor uw slimme gebouwen;
- het testen van de beveiliging van de systemen in slimme gebouwen.

Vier aandachtspunten voor smart building security

Toegang tot het smart building-netwerk en de domotica: slimme gebouwen zijn vaak benaderbaar vanaf het internet - dit stelt gebruikers en bewoners in staat om via Apps op afstand bedieningsfuncties uit te voeren, om intelligente stemassistenten in te zetten, en om data te ontsluiten naar dashboards en andere verbonden systemen. Daarom moet toegang tot het netwerk goed zijn beveiligd, zodat alleen de rechtmatige gebruikers er toegang tot kunnen verkrijgen. Gebruik veilige verbindingsprotocollen en sterke authenticatie om een adequaat beveiligingsniveau af te dwingen.

Veilige domotica: domotica is enorm in ontwikkeling en er is een enorm aanbod aan systemen in de markt. Ook op het gebied van beveiliging verschilt het aanbod enorm. Een onveilig domoticasysteem kan toegang bieden tot het gehele smart building-netwerk. Gebruik daarom alleen vertrouwde en mogelijk gecertificeerde leveranciers en producten. Test eventueel de beveiliging van systemen, voordat u ze in uw gebouwen plaatst.

Bedrijfsvoering en processen: Informatiebeveiliging is niet alleen een technische aangelegenheid - onjuiste bedrijfsvoering en procesgang kan ook leiden tot datalekken en ongeautoriseerde toegang tot systemen. Richt daarom veilige processen in omtrent het verlenen en ontnemen van toegang tot data en systemen, voor het herkennen van oneigenlijk gebruik en voor het tijdig identificeren van beveiligingsrisico's in de slimme gebouwen.

Privacy: de data die wordt verzameld en verwerkt door slimme gebouwen zegt mogelijk enorm veel over het gedrag en de persoonlijke levenssfeer van de gebruikers en/of bewoners. Daarom is geldende privacy wet- en regelgeving van toepassing op (aspecten van) de uw slimme gebouwen. Analyseer welke specifieke regels op uw smart building-systeem van toepassing zijn middels een Privacy Impact Assessment en richt vervolgens de juiste maatregelen in.

Contact

Voor meer informatie over Smart Building Security, of KPMG's Cyber Security-dienstverlening, kunt u ons bezoeken op:https://www.kpmg.com/nl/cyber

Of neem contact op met onze specialisten:

Mark Poen
T +31 (0)6 20 44 53 30
poen.mark@kpmg.nl

Sander Grunewald
T. +31 6 50692013
grunewald.sander@kpmg.nl

Paul van Iterson
T +31 (0)6 46 74 86 35
vaniterson.paul@kpmg.nl

KPMG on socialmedia

Available on the App Store

KPMG app

KPMG
Laan van Langerhuize 1
1186 DS Amstelveen

kpmg.nl