Rijksgebouwen beschermen tegen cyberaanvallen

Een stevige klus voor de specialisten van het Rijksvastgoedbedrijf

De gebouwen van de Rijksoverheid hangen vol met sensoren, brandmelders, beveiligingssystemen en beheerinstallaties. Al die installaties en systemen zijn dankzij de snel toenemende digitalisering steeds meer met elkaar verbonden. Én met de buitenwereld. Dat brengt risico's met zich mee. Rinke, coördinator cybersecurity bij het Rijksvastgoedbedrijf (RVB), vertelt over de uitdagingen en hoe zij risico's voorblijven.

Kantoren, defensievastgoed, paleizen, rechtbanken, gevangenissen en het Binnenhof: het Rijksvastgoedbedrijf beheert en onderhoudt al het vastgoed van de Rijksoverheid. Meer dan 12.000 gebouwen zijn het, door het hele land. En in die gebouwen bevindt zich een immense hoeveelheid installaties. Die zijn nodig voor het dagelijks functioneren, maar bijvoorbeeld ook voor de beveiliging en bij calamiteiten. Wat als zo'n systeem verstoord wordt door een cyberaanval?

Voor de lol of met kwade bedoelingen. "Dat is zeker geen hypothetische situatie", zegt Rinke. "Hackers hebben interesse in de technologieën in gebouwen. Met cyberaanvallen kunnen ze systemen beïnvloeden, platleggen en informatie ontvreemden. Voor de lol, zoals jongens en meiden op hun zolderkamer die het gaaf vinden om te kijken hoever ze kunnen komen. Of vooropgezet, bij doelgerichte acties van kwaadwillende hackers". Wie het ook

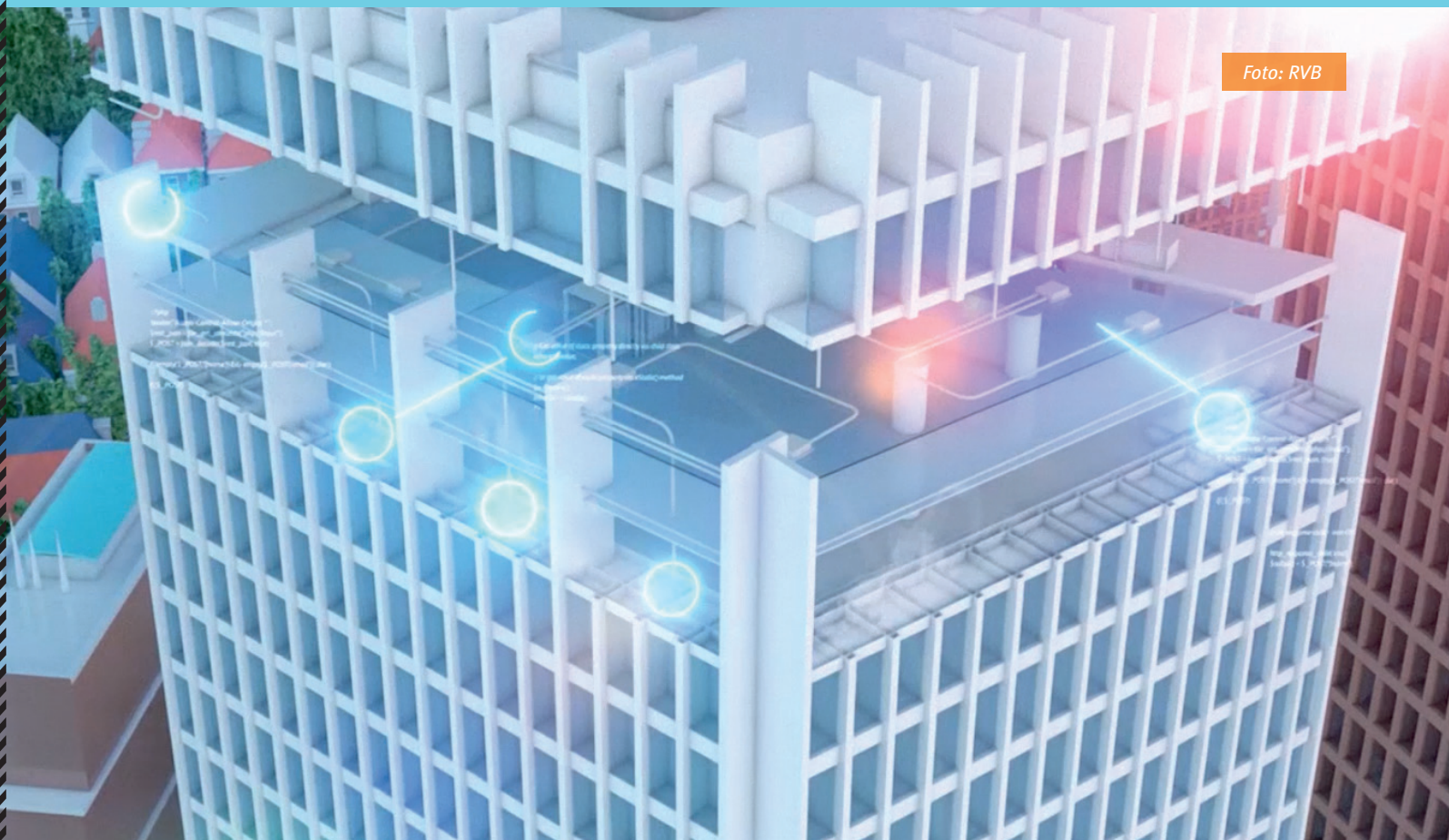

Foto: RVB

Foto: RVB

veroorzaakt, een verstoring of uitval van de systemen kan grote gevolgen hebben. “Een aanvaller heeft maar één opening nodig, wij moeten op alle vlakken verdedigen”. Digitale aanvallen zie of hoor je niet, totdat ze slagen en schade aanrichten. Het Rijksvastgoedbedrijf investeert flink in bescherming tegen internetinbraak. “Want”, zegt Rinke, “een aanvaller heeft maar één opening nodig, wij moeten op alle vlakken verdedigen”. Dus werken de cybersecurityspecialisten van het RVB dagelijks aan het versterken en uitbouwen van de digitale bescherming van de systemen in alle rijksgebouwen.

Nooit one size fits all. Dat is een uitdagende opdracht. “Vooral omdat we te maken hebben met een grote diversiteit aan systemen, en dus met verschillende ontwerpen, technologieën en volwassenheidsniveaus. En met een keur aan leveranciers, type gebouwen en gebruikers. Het is bij ons nooit one size fits all. Toch proberen we zoveel mogelijk te standaardiseren en te werken vanuit eenzelfde basis. We werken met ICT-achtige systemen, die draaien op servers en IP-netwerken. Maar ook met operationele technologie (OT), zoals brandmeldcentrales en gebouwbeheersystemen. Die hebben weer specifieke protocollen en ze moeten voldoen aan specifieke eisen. Bij rookvorming moet er bijvoorbeeld nú een alarm afgaan, en niet over vijf minuten”.

En dan is er nog de omgeving waarin een systeem gebruikt wordt. “Een ogenschijnlijk simpele installatie als een intercom heeft in het ene gebouw een totaal andere functie dan in het andere. Als de knop niet goed werkt bij een kantoorentree is dat hooguit onhandig. Maar in een gevangenis is de intercom in de cel de levenslijn van de gedetineerde. Werkt hij niet, dan is er een groot veiligheidsrisico. “We digitaliseren voortvarend, en dat is logisch omdat het veel zaken makkelijker maakt. Maar het maakt ook kwetsbaarder. Want systemen zijn steeds meer met elkaar verbonden, en met de buitenwereld. Alles beïnvloedt elkaar en kan elkaar verstoren”.

Een groot aanvalsoppervlak. “Die connectie met de buitenwereld is een groot ‘aanvalsoppervlak’, zoals we dat noemen. Net als mensen die in het gebouw werken: onderhoudsprofessionals, facilitymedewerkers en technici. Zij moeten in de systemen zijn, werken ermee of dicht in de buurt en kunnen ze onklaar maken - per ongeluk of met opzet. Daarnaast kunnen ook de leveranciers van onze systemen getarget worden. Als hun beveiliging kwetsbaar is, is dat ook een risico voor onze systemen”.

Altijd een stap voor. Waar te beginnen, om al die risico’s het hoofd te bieden? “We werken er doorlopend aan om mogelijke risico’s in kaart te hebben en ons vastgoed ertegen te beschermen. We moeten in feite altijd een stap voor zijn op mogelijke aanvallers. We werken met ons Cybersecurity Raamwerk Vastgoed. Wat ons betreft wordt dit dé standaard voor cybersecurity in vastgoed. We hanteren andere uitgangspunten dan in de bekende beveiligingsprotocollen. Een voorbeeld? Het bekende ‘3 keer een verkeerd wachtwoord ingevoerd? Dan wordt de toegang geblokkeerd’, kun je niet toepassen in een meldkamer. De man of vrouw die daar ’s nachts aan het werk is, moet te allen tijde doorkunnen”.

Rinke Andriessen Foto: RVB

Hoe houden we de balans tussen veiligheid en goed en snel functioneren? Beveiligingsmaatregelen neemt het RVB dan ook naar gelang het risico, het type gebouw en het belang van een systeem voor de gebruiker en de omgeving. “We stellen onszelf steeds de vraag: hoe erg worden we geraakt als een systeem uitvalt? En hoe houden we de balans tussen veiligheid en goed en snel functioneren? Versleuteling bijvoorbeeld, is veiliger maar geeft vertraging en dat wil je niet bij alle systemen. De vitale systemen hebben altijd voorrang. We maken ze nog betrouwbaarder en stabieler door ze een dubbele stroom- of netwerkaansluiting te geven, of door ze zelfs helemaal dubbel uit te voeren”.

Complexe, maar o zo interessante materie. Risico’s zijn en blijven onderdeel van het werk van Rinke en zijn collega’s. Een van de grootste risico’s is volgens hem dat we afhankelijker zijn van systemen dan we denken. “Veel mensenwerk wordt overgenomen door systemen die ons helpen. Maar wat gebeurt er als die systemen ineens wegvallen? Daar moeten we ons veel meer bewust van zijn. Ik begrijp ook wel dat het zo werkt hoor. Het is complexe materie, lastig om over na te denken. Maar voor mijn collega’s en mij heel wezenlijk en elke dag weer uitdagend. We zijn enorm gemotiveerd om steeds te verbeteren en dingen slimmer en efficiënter te doen”.

Kijken naar het grote geheel. Een goede stap vooruit is om zaken minder per pand of per installatie aan te pakken, maar meer te kijken naar een groter geheel. “Het wordt voor onszelf en voor de markt gemakkelijker als we nadenken over het gelijktrekken van ontwerpen, protocollen en netwerken. We proberen binnen het Rijksvastgoedbedrijf al zoveel mogelijk projectoverstijgend te werken. Voor een aantal panden tegelijk, met beheer op een centrale plek. Zo leren we intern veel van elkaar en gebruiken we elkaars kennis waar we kunnen”.

Samen met leveranciers. “Ook praten we regelmatig met brancheorganisaties en leveranciers. Over trends, ontwikkelingen en nieuwe oplossingen op het gebied van cybersecurity, en hoe die te vertalen naar onze specifieke situatie. Soms hebben we lastige gesprekken met leveranciers om te komen tot een goede, ‘cybersecure’ oplossing. Maar het is mooi als je ziet hoe ze diezelfde oplossing gemakkelijker toepassen in een volgend project. Het geeft energie dat we elkaar zo steeds verder versterken”.

Meer weten over de aanpak van cybersecurity bij het Rijksvastgoedbedrijf?

‘Als een intercom bij een kantoorentree niet werkt, is dat onhandig. In een gevangenis kan het gevaarlijk zijn’