WAAROM SECURITY BELANGRIJKER IS DAN OOIT (EN HOE JE CYBERAANVALLEN VOORKOMT)

Je leest het regelmatig in de krant of hoort het op de radio: wéér een bedrijf slachtoffer van een grote cyberaanval. Belangrijke data gestolen, duizenden euro's verlies en een flinke emotionele klap voor alle betrokkenen. Toch weet jouw bedrijf de dans telkens weer te ontspringen. Dat zal wel zo blijven, toch?

Volgens Rik Maassen, IT-directeur van CTS IT, is het niet een kwestie van óf je slachtoffer wordt van hackers, maar wanneer. Gelukkig kun je met de juiste IT-voorzieningen ervoor zorgen dat je cybersecurity op orde is. Zoals al gezegd kunnen we een hack niet 100% voorkomen maar verkleinen we de kans, als ze vervolgens toch binnen komen zorgen we ervoor dat we de impact minimaliseren. Daarom werken we bij CTS IT proactief voor onze klanten. We zoeken en versterken de zwakke plekken in je IT-omgeving, nog voor ze bekend zijn bij kwaadwillenden."

CYBERSECURITY

Security of cybersecurity is een verzamelterm voor alle maatregelen die je treft in je organisatie om te voorkomen dat je slachtoffer wordt van virusaanvallen, DDoS-aanvallen, phishing en meer. Ransomwareaanvallen hebben met name een gigantische impact op bedrijven: dan wordt er belangrijke data gestolen en gegijzeld. Alleen door geld te betalen krijg je die belangrijke data (als het goed is) terug van de hackers.

IMPACT VAN CYBERAANVALLEN

Rik Maassen legt uit dat de impact van cyberaanvallen veel verder gaat dan omzetverlies. "De data die is buitgemaakt moet je vaak terugkopen, wat nog meer kosten met zich meebrengt. Maar dat is nog maar een tipje van de sluier. Je kunt een cyberaanval zien als een hartaanval voor je bedrijf. Alles en iedereen om dat hart heen ondervindt de consequenties. Klanten gaan misschien wel op zoek naar een andere dienstverlener omdat je langere tijd niet kunt voldoen aan werkafspraken. Medewerkers voelen zich verantwoordelijk of zijn bang hun baan te verliezen. Als ondernemer krijg je emotioneel ook een flinke klap. Er komt dus veel meer leed bij kijken dan je verwacht."

MAATREGELEN OP DRIE FRONTEN

Om klanten weerbaar te maken tegen die aanvallen, pakt CTS IT cybersecurity aan op drie fronten: data, gebruikers en device. Rik legt uit: "We nemen maatregelen om je data goed te verbergen en versleutelen, bijvoorbeeld door documenten te labelen en bestandsdeling te beperken. Daarnaast zorgen we ervoor dat je devices - oftewel je apparaten - veilig zijn met de nieuwste software en opties als meervoudige verificatie (MFA) bij inloggen.

Het stuk van de gebruiker is misschien wel het belangrijkste, maar wordt ook het meest over het hoofd gezien. Een gebrek aan bewustzijn over hoe je veilig werkt in een IT-omgeving kan ervoor zorgen dat er een digitaal deurtje open staat in je organisatie. Als een hacker die achterdeur weet te vinden, ben je al snel slachtoffer van een aanval." Overigens kan zo'n open achterdeurtje volgens Rik ook het gevolg zijn van bijvoorbeeld verouderde systemen.

CREËER BEWUSTZIJN IN JE ORGANISATIE

Die eindgebruiker is dus een belangrijke spil in je security. Toch zijn er veel ondernemers die het belang van IT-awareness bij medewerkers niet goed op het netvlies hebben. "Ze vinden het nog altijd een spannend idee om werknemers regelmatig tijd te laten investeren in training over security, ten koste van ander werk dat moet gebeuren. Toch is bewustwording over IT-gevaren van groot belang als je écht veilig wil zijn."

Maar hoe creëer je een cyberawareness-cultuur in je organisatie? Dat kan volgens Rik op verschillende manieren. "Er zijn allerlei trainingen die je personeel kan volgen waarmee ze een opfrisser krijgen over de nieuwste ontwikkelingen en gevaren in IT. Dat kan ook in de vorm van een spelletje of quiz."

AWARENESS ON THE JOB

Het meest effectieve is volgens Rik wat hij noemt awareness on the job: dan wordt bewustwording creëren over IT-gevaren een onderdeel van je dagelijkse werk. CTS IT stuurt dan bijvoorbeeld een mail naar iedereen in de organisatie, in overleg met de klant en zonder medewerkers op de hoogte te brengen. "Dat is een valse e-mail die de lezer uitnodigt op een link te klikken, zogenaamd naar een betaling of andere handeling. In feite is het onze versie van een phishingmail of ethical hacking."

"Als de lezer op de link klikt, wordt hij direct geconfronteerd met zijn actie. Daar leest hij een toelichting op de mail en geven we een stukje voorlichting over zijn actie en de gevolgen. Zoiets gebeurt gewoon door je dagelijkse werkdag heen. We zien dat zo'n grootschalige mailgolf extra veel impact maakt op mensen. Het zet ze aan het denken. Je kunt iemand immers tien keer vertellen dat hij niet te hard mag rijden, maar als hij bijna een fietser onder z'n auto heeft, maakt dat veel meer impact."

DE BALANS TUSSEN GEBRUIKSGEMAK EN IT-VEILIGHEID

In principe kun je bij elke IT-leverancier aankloppen om je security aan te pakken. CTS IT gaat een stap verder. "We benaderen klanten proactief en denken mee met wat je nodig hebt, nog voor je het zelf weet. Bovendien houden we de balans tussen gebruiksgemak en veiligheid goed in de gaten. Dat is cruciaal. Hoe zorg je dat je IT-omgeving veilig is, maar de eindgebruiker toch zo weinig mogelijk hinder ondervindt en zijn werk goed kan doen? Dat zoeken wij voor je uit. Veiligheidsmaatregelen moeten namelijk ook bijdragen aan je bedrijfsprocessen en je werk makkelijk maken. Daar zorgen wij voor."

DE TOEKOMST VAN CYBERSECURITY

IT verandert snel. Cybersecurity dus ook. Daarom kijken ze bij CTS IT altijd vooruit, vertelt Rik. "We houden de markt en ontwikkelingen nauw in de gaten voor onze klanten."

"Op korte termijn krijgen veel bedrijven bijvoorbeeld te maken met de NIS 2.0. Dat zijn nieuwe wetten en richtlijnen vanuit de Europese Unie voor veilige digitale omgevingen. De komende jaren moeten veel bedrijven daardoor niet alleen hun software, maar ook hun hardware updaten of vervangen. Bij CTS IT weten we waar je aan moet voldoen voor die NIS 2.0. We adviseren, maken samen een meerjarenplan en leggen uit waar je het beste kunt investeren. Een ding is zeker als het deze ontwikkeling betreft: je kunt beter gisteren handelen dan vandaag."

OOK JE SECURITY OP ORDE?

CTS IT is de partij die je proactief helpt om cyberincidenten te voorkomen. Zodat jij veilig bent en blijft. Nu en in de toekomst, wat je ook staat te wachten op het gebied van IT. Neem via www.cts-it.nl/contact/ contact op en laten we elkaar leren kennen.