Alarmerend nieuws: stad Antwerpen slachtoffer van een ransomware-aanval

20 december 2022, 10:18

Tatiana Galibus

Vorige week werd de stad Antwerpen het slachtoffer van een ransomware-cyberaanval. Ransomware is een computervirus (malware) dat gebruikmaakt van encryptie om het slachtoffer geld afhandig te maken. Het versleutelt de kritieke gegevens van een gebruiker of bedrijf om de toegang tot bestanden, databases of toepassingen te blokkeren. Er wordt dan losgeld gevraagd om opnieuw toegang te verlenen.

De meeste openbare diensten van Antwerpen liggen nu stil, inclusief de e-diensten van de stad, musea en bibliotheken. De aanval wordt opgeëist door Cyber Play op zijn website op het dark web. Het lijkt om een nieuwe bende te gaan die niet voorkomt in het Kaspersky-rapport, een lijst van de 8 gevaarlijkste ransomware-virussen ter wereld. Dit bewijst maar weer dat zelfs kleinere cybercriminelen ernstige schade kunnen aanrichten, dat machten snel kunnen verschuiven en bedreigingen kunnen ontstaan in de cyberwereld.

Kan de cyberveiligheid van Belgische bedrijven vandaag worden gegarandeerd?

Het antwoord is ‘nee’, zo simpel is dat. Ransomware-bendes zijn goed georganiseerd. Soms beter dan de bedrijven die ze aanvallen. En ze maken graag gebruik van ouderwetse technologieën: phishing, spear phishing, USB-sticks enz. En zoals uit de aanval van vorige week blijkt, werken deze methoden nog steeds.

Waarom? Omdat men in het geval van zo'n georganiseerde bende niet te maken heeft met een programma of een script, maar met een goed geolied netwerk van cybercriminelen met elk hun specifieke vaardigheden, die allemaal hetzelfde doel willen bereiken. De beruchte lekken van de Conti-bende, de ‘Panama Papers of Ransomware’, toonde ons de modus operandi en interne werking van zo'n bende.

> Wist u dat een Belgisch bedrijf gemiddeld meer dan 3000 cyberaanvallen per jaar te verwerken krijgt? En alleen al in 2022 was er een stijging van 28%. Hoogtijd dus om actie te ondernemen.

De cyberbeveiligingscultuur is een must

Het is belangrijk dat bedrijven er een duidelijke en precieze cyberbeveiligingscultuur op nahouden. Om in deze snel veranderende wereld beschermd te zijn, moet u, als manager, zonder aarzelen de volgende basisvragen kunnen beantwoorden:

- Weten al mijn werknemers wat phishing is? Weten ze hoe het werkt, wat de mogelijke signalen kunnen zijn van een phishing-poging?
- Ben ik er zeker van dat niemand in mijn bedrijf uit nieuwsgierigheid die dodelijke klik gaat doen of die USB-stick in een computer gaat steken?
- Hebben we een duidelijke toegangsstrategie en -controle?
- Worden onze gevoelige gegevens apart opgeslagen op een gecodeerd opslagmedium?

Moet u op veel vragen negatief antwoorden?Hebt u veel twijfels? Dan moet u dringend prioriteit geven aan uw cyberbeveiliging.

Sirris kan u daarbij helpen

De komende maanden organiseren we 2 leertrajecten in cyberbeveiliging voor digitale diensten en manufacturing. Beide leertrajecten behelzen zowel diepgaande theoriemodules als praktijksessies op maat. We werken samen met partners die gespecialiseerd zijn in cyberbeveiliging om u de beste lessen én netwerkingervaring te bieden. Bovendien krijgt u verschillende **micro-coachingsessies voor uw specifieke problemen.**

Auteurs

Tatiana Galibus