

Toekomstbestendige cybersecurity, ook voor kmo's!

14 september 2021, 02:00

Annanda Rath

Tatiana Galibus

In tijden van digitale transformatie en Industrie 4.0 is cybercriminaliteit nog nooit zo reëel geweest voor Belgische kmo's. Elk bedrijf dat niet over voldoende beveiligingsveerkracht beschikt is een potentieel slachtoffer. Kmo's hebben een strategie op maat en een duidelijk stappenplan nodig om zichzelf te beschermen, nu en in de toekomst. Sirris en Agoria komen u tegemoet met een nieuwe aanpak, afgestemd op kmo's!

Cybercriminaliteit is nog nooit zo reëel geweest voor Belgische kmo's, nu grote bedrijven niet langer het enige doelwit van cybercriminelen zijn. Momenteel zijn er meer dan 30.000 cyberaanvallen geregistreerd met een jaarlijkse stijging van 20 procent van het aantal incidenten. De digitale transformatie en Industrie 4.0 vormen een groot risico voor ondernemingen, omdat verouderde machines met een hoog beveiligingsrisico verbonden zijn en data verzameld en uitgewisseld worden tussen websites zonder enige controle. Elk bedrijf dat niet beschikt over voldoende beveiligingsveerkracht kan slachtoffer worden van cybercriminaliteit en de gevolgen van beveiligingsinbreuken - onderbreking van activiteiten, gegevensverlies en een reputatiebeschadiging - kunnen een bedrijf onderuithalen, met vaak grote gevolgen op korte en langere termijn.

Om zich tegen dergelijke aanvallen te beschermen hebben kmo's uit de verschillende sectoren een eigen aanpak nodig en dit is wat Sirris en Agoria hebben uitgewerkt binnen een breed aanbod met zeer gerichte en praktische workshops, aangepast aan de doelgroep, sector en het type bedrijf.

Van intake tot cyberbeveiligingsscan

Sirris heeft een nieuwe flexibele aanpak van cyberbeveiliging ontwikkeld om kmo's te helpen bij het realiseren van hun cyberbeveiligingsstrategie, zonder al te veel moeite en financiële middelen te investeren. We starten hierbij met een **gratis online intake sessie** van 1 uur. Na deze sessie zorgen we voor een gestructureerd rapport met de reeds gedetecteerde problemen en geven daarbij ons advies over hoe deze problemen aan te pakken. Het bedrijf kan op basis van de aanbeveling(en) in dit document onmiddellijk beginnen met het verbeteren van de algemene cyberbeveiliging.

Wil het bedrijf nog een stap verder gaan en wenst het een **diepgaandere cyberbeveiligingsscan**, dan komen we ter plaatse en gaan we veel dieper in op alle afzonderlijke punten op basis van de resultaten van beveiligingsscan's en interviews. Het resultaat van de scan levert een gestructureerde tabel op van bedrijfsmiddelen, kwetsbaarheden en risico's. Het bedrijf kan op die manier makkelijker een beslissing nemen over de volgende te nemen stappen en prioriteiten voor een veerkrachtigere cyberbeveiliging.

Lees [hier](#) meer over deze aanpak.

Workshops voor elk type bedrijf uit elke sector

Op zoek naar concrete tips & tricks voor cybersecurity?

Wij helpen u een digitale lockdown van uw bedrijf (of erger) voorkomen tijdens de no-nonsense, uiterst praktische **masterclass 'Cyberveilig in 30 stappen'**. We bespreken een risico-gebaseerde aanpak die een fundamentele basis zou moeten vormen voor elk bedrijf en richten op hierbij op de cyberveiligheid van de interne werkmiddelen. We leggen u 30 haalbare en onmiddellijk toepasbare stappen uit, waarmee u de cyberveiligheid in uw bedrijf naar een aanzienlijk hoger niveau kunt tillen. Als u deze 30 stappen goed toepast, zal u al een hele mooie balans gevonden hebben tussen het risico dat u loopt en de investering die u in cybersecurity doet.

Als maakbedrijf uw weg vinden in cybersecurity?

Cyberveiligheid is voor veel productiebedrijven een heet hangijzer. Lacunes in de cyberveiligheid kunnen leiden tot het verlies van data, financiële verliezen en reputatieschade. Het **webinar 'Cyberveiligheid voor maakbedrijven'** stelt de belangrijkste cyberveiligheidsoplossingen voor en licht de optimale praktijken toe om de cyberveiligheid in de productie te verbeteren, uit zowel IT- als OT-oogpunt (informatietechnologie en geconnecteerde werkvloer). Dit webinar spitst zich toe op pragmatische oplossingen die ook voor kmo's haalbaar zijn.

De **masterclass 'Cybersecurity voor maakbedrijven'** leert u hoe veilig stappen te nemen richting Industrie 4.0 via een uitvoerbare stapsgewijze roadmap naar veerkrachtige cyberveiligheid. We reiken u de kennis aan in een pragmatisch hands-on format en brenen u zo een diepgaand inzicht in alle veiligheidsaspecten van uw transitie naar Industrie 4.0.

Op basis van de resultaten van de studie '[Cyberveiligheid in de Belgische Maakindustrie](#)' besloten Sirris en Agoria om maakbedrijven samen te brengen in een **lerend netwerk rond het thema van cybersecurity in OT**, meer bepaald het kunnen detecteren van dreigingen en anomalieën in de productieomgeving. Het significant verbeteren van de detectiemogelijkheden is immers in veel gevallen een van de minst ingrijpende manieren om de cyber-weerbaarheid van de productieomgeving aanzienlijk te verhogen.

Hoe als digitale startup of scale-up security assessments overleven?

Als startup of scale-up, na maanden van demo's en dergelijke, al op negatief advies van TPSA-assessors binnen een groot bedrijf gebotst? Risico management en de 'trust decision' komen maar al te vaak op het einde van de buyer journey en onvoldoende vertrouwen is dan de belangrijkste reden waarom het ultiem toch nog misloopt. Over dit 'TPSA'-domein valt nog heel wat te leren, van elkaar én vanuit het perspectief van zo'n assessor. Daarom brengen we een groep digitale product- en servicebedrijven samen in een **lerend netwerk rond het thema van het overleven van zo'n security assessment**.



(Bron beeld banner: iStock)

Auteurs



Annanda Rath



Tatiana Galibus