



Cybersecurity 4.0: resultaten enquête naar cyberbeveiligingsbehoeften van maakbedrijven

30 maart 2023, 15:29

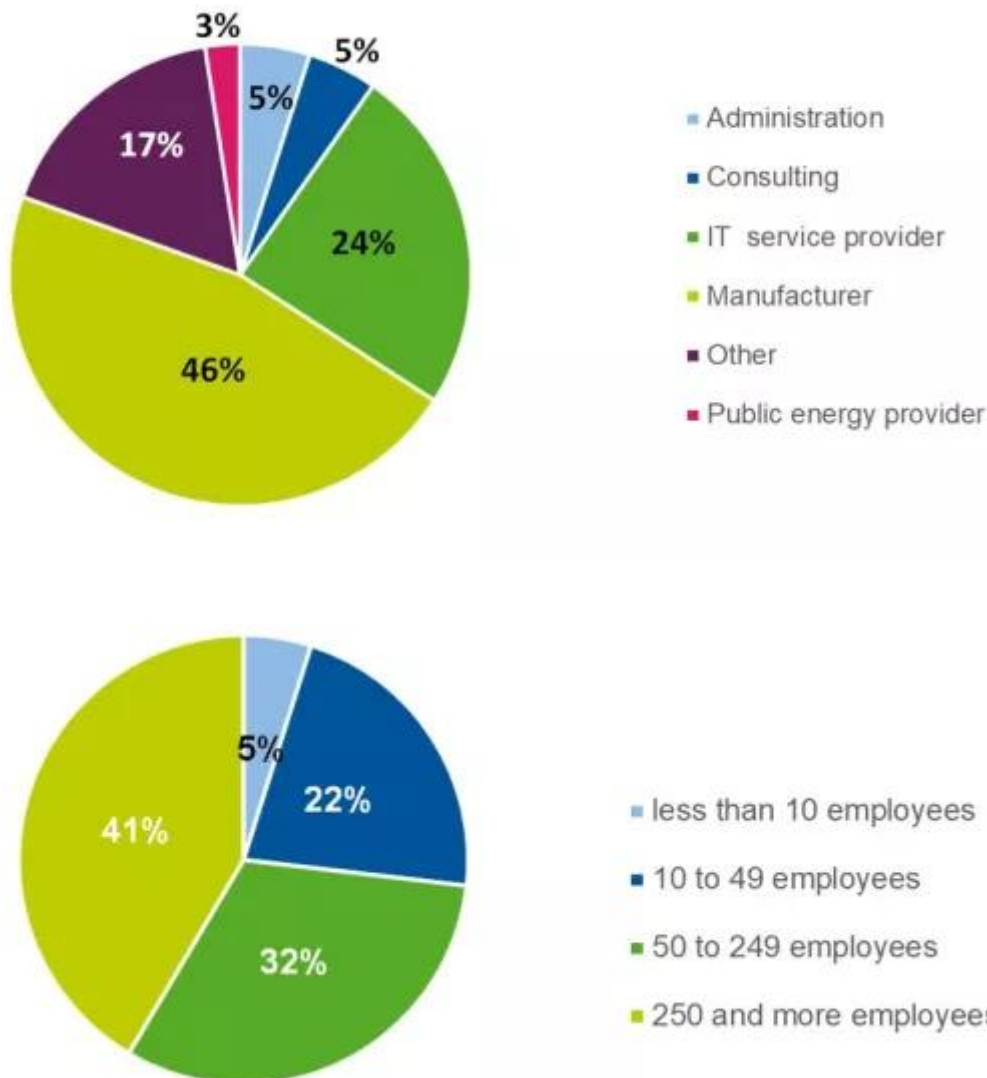
Tatiana Galibus
Annanda Rath

In het kader van het onderzoeksproject Cybersecurity 4.0 hebben we van maart tot oktober 2022 een enquête gehouden bij Belgische en Duitse maakbedrijven. In deze blogpost delen we graag enkele interessante resultaten en tendensen uit deze enquête.

Het onderzoeksproject [Cybersecurity 4.0](#) wil kmo's een haalbaar raamwerk en een leeromgeving voor cyberbeveiliging bieden, met focus op connectiviteit, databeveiliging en beveiliging van de toeleveringsketen.

Analyse van de testcases en gebruikerseisen

41 bedrijven werden geïnterviewd of bevraagd.



We hebben de enquêteresultaten geanalyseerd aan de hand van een statistische classificatie-, score- en ratingmethode. Als resultaat van de enquête hebben we **drie grote bedrijfsprofielen** afgebakend: maakbedrijven, kmo's en serviceproviders. We hebben **11 belangrijke beveiligingsdomeinen** geïdentificeerd waarmee bedrijven rekening moeten houden bij de implementatie van cyberbeveiliging, waaronder netwerk- en databeveiliging, beveiliging van de toeleveringsketen, toegangscontrole en OT/IOT-beveiliging.

Veiligheidsrisico's bij de maakbedrijven

We hebben de **grootste veiligheidsrisico's** voor maakbedrijven uitgelicht: talrijke kritieke domeinen vertonen gebreken, onder meer op het vlak van toegangscontrole, dataclassificatie, training in cyberbeveiliging en beoordeling van de veiligheidsrisico's bij de partners in de toeleveringsketen. Van de 20 bedrijven die we hebben bevraagd en die de online enquête hebben beantwoord (hetzij 46%), zijn er 13 die hun data niet classificeren, 11 die de toegang tot hun systeem en netwerk niet controleren en 8 die hun back-ups niet encrypten. Meer dan 50% van de bedrijven (12) beoordeelt het veiligheidsrisico bij hun partners in de toeleveringsketen niet en 10 bedrijven hebben geen trainingsprogramma's in cyberbeveiliging, wat nochtans als een belangrijke factor voor cyberveiligheid wordt beschouwd.

Deficit	Frequencies	Comments
No back up encryption	8	+ 1 "Not specified"
No access control	5	+ 1 "Don't know"
No audit of access control	11	-
No data classification	13	+ 1 "Don't know"
No network segmentation	13	+ 1 "Not specified"
No network monitor	5	+ 2 "Don't know"
No cyber security training	6	+ 1 "Don't know"
No implementation standards for cyber security training	6	-
No risk assessment for supply chain partners	10	+ 2 "Don't know"
	12	+ 7 "Not specified"
		+ 2 "Don't know"

Tabel 1. Lijst van de beveiligingsgebreken bij de bevraagde maakbedrijven

Veiligheidsrisico's bij de serviceproviders

Bij de serviceproviders zien we een relatieve verbetering op het vlak van beveiliging. Er zijn echter nog enkele gebreken in kritieke domeinen, zoals toegangscontrole, dataclassificatie en beoordeling van de veiligheidsrisico's bij hun partners in de toeleveringsketen. 5 op de 10 bedrijven (of 24%) hebben nog steeds geen degelijk toegangscontrolesysteem of optimale praktijken, en 7 op de 10 bedrijven hebben geen beoordeling van de veiligheidsrisico's voor hun partners in de toeleveringsketen. 4 bedrijven hebben geen trainingsprogramma's in cyberbeveiliging, wat

Deficit	Frequencies	Comments
No backup encryption	1	+ 4 "Not specified"
No access control	5	+ 1 "Not specified"
No audit of access control	5	+ 1 "Not specified"
No data classification	5	+ 1 "Don't know"
No network segmentation	5	+ 1 "Not specified"
No network monitor	2	+ 1 "Not specified"
No cyber security training	3	+ 2 "Not specified"
No implementation standards for cyber security training	3	+ 1 "Don't know"
No mitigation plan	4	
No risk assessment for supply chain partners	4	+ 4 "Not specified"
	4	+ 1 "Don't know"
	4	+ 2 "Not specified"
	7	-

Tabel 2. Lijst van beveiligingsgebreken bij de serviceproviders

Veiligheidsrisico's bij de kmo's

59% van de 41 bedrijven die we hebben bevraagd en geïnterviewd, zijn kmo's (m.a.w. bedrijven met minder dan 250 werknemers). We stellen een gelijkaardige trend vast met betrekking tot de beveiligingsgebreken, gaande van toegangscontrole, dataclassificatie, netwerkmonitoring, training in cyberbeveiliging en risicobeperkingsplan tot beoordeling van de veiligheidsrisico's bij de partners van de toeleveringsketen.

Deficit	Frequencies	Comments
No backup encryption	-	+ 1 "not specified" + 1 "don't know"
No access control	3	+ 1 "don't know"
No audit of access control	4	+ 1 "don't know"
No data classification	4	+ 1 "don't know"
No network segmentation	4	-
No network monitor	2	+ 1 "don't know"
No cyber security training	3	-
No implementation standards for cyber security training	3	+ 2 "not specified" + 2 "don't know"
No mitigation plan	2	+ 2 "don't know"
No risk assessment for supply chain partners	4	+ 1 "don't know"

Tabel 3. Lijst van beveiligingsgebreken bij de kmo's

Specificatie van het maturiteitsmodel, kwetsbaarheids- en risicoanalyse

We werken momenteel aan de specificatie van de maturiteitscriteria van de cyberbeveiliging met betrekking tot het bedrijfsprofiel en het risico. Van zodra we een efficiënt en relevant model hebben reformuleerd, zullen we de cyberbeveiliging van de bedrijven kunnen indelen op een schaal van 1



In april zullen Sirris en FIR Aachen de enquêtevragen publiceren, zodat elk bedrijf ze online kan beantwoorden.

In een volgende stap zullen we een **raamwerk, een webtool en richtlijnen** ontwikkelen als toekomstig webplatform om cyberbeveiliging te ondersteunen. Er zal een **demonstrator** worden geïmplementeerd, in de vorm van een geconnecteerde productielijn, die **typische aanvalsscenario's en risicobeperkingen** simuleert voor verschillende beschermingsniveaus, waaronder diverse beveiligingsmaatregelen en -configuraties.



huidige demonstratoropstelling

Samen op weg naar Cybersecurity 4.0

Het project-Cybersecurity 4.0 is bedoeld om bewustmaking- en verspreidingstools te ontwikkelen. Bent u geïnteresseerd in een bepaald aspect van cybersecurity? Wilt u de resultaten in detail bekijken? Of een gesprek met ons of met andere Belgische bedrijven opzetten? [Neem contact met ons op!](#)

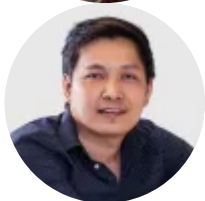
Eind april organiseren we een videoconferentie van het Belgische consortium, een webinar voor de gebruikersgroep of specifieke vraag-en antwoordsessies. Op **27 april** start Sirris met een pragmatisch opleidingstraject van 2 maanden om maakbedrijven te helpen met hun cyberbeveiliging. [Schrijf u in!](#)

We bieden ook individuele coachingsessies en masterclasses bij u ter plaatse, om u te helpen uw eigen cyberbeveiligingsstrategie te ontwerpen en specifieke risico's uit de weg te ruimen. [Raadpleeg ons collectieve en individuele aanbod!](#)

Auteurs



Tatiana Galibus



Annanda Rath