hoppenbrouwers

Goed bezig!

Je hebt de test gedaan!
Heb jij je OT-risico's goed in kaart?

Ontdek wat de uitslag van de test betekent en wat
de volgende stap is naar een veilige OT-omgeving.

Introductie

De eerste stap is gezet! Je hebt de test ingevuld en inzicht gekregen in de huidige staat van je OT-risico's.

Dit advies helpt je te begrijpen wat je huidige score betekent en hoe je verder kunt gaan om je risico's in kaart te brengen en je OT-omgeving te beveiligen. Hier vind je praktische stappen die je direct kunt ondernemen om de veiligheid van je systemen te verbeteren.

Score-inzicht:

Op basis van je score heb je nu een beter beeld van hoe goed je je OT-risico's in kaart hebt.

Lees op de volgende pagina's wat jouw testuitslag betekent en hoe je hiermee aan de slag kan.

13 - 15 punten

Lekker bezig!!

Wat betekent dit voor jou?

Je hebt je risico's grotendeels in kaart en hebt al veel goede maatregelen getroffen om je OT-omgeving te beschermen.
Het is belangrijk om periodiek te blijven evalueren en bij te stellen. Cyberdreigingen veranderen voortdurend, dus blijf op de hoogte van nieuwe kwetsbaarheden.

Wat kun je doen om verder te verbeteren?

- Blijf regelmatig je systemen monitoren en bijwerken. Zet bijvoorbeeld een blok in je agenda iedere zoveel maanden om alles te checken.
- Zorg ervoor dat je risicoanalyses up-to-date blijven en alle nieuwe componenten of veranderingen in je OT-omgeving worden meegenomen.
- Onderhoud een goede communicatie met je leveranciers over beveiligingkwesties. Maak een beveiligingscheck ook onderdeel van de checklist wanneer er een nieuw contract getekend wordt met een nieuwe leverancier.

Praktische tips!

Bijhouden van kwetsbaarheden:
Gebruik tools voor automatische monitoring van kwetsbaarheden zoals CVE-databases. Zorg ervoor dat deze continu worden bijgewerkt.

Regelmatige audits:
Voer periodieke interne en externe audits uit om de effectiviteit van je beveiligingsmaatregelen te testen. Zet bijvoorbeeld een blok in je agenda iedere zoveel maanden om alles te checken.

Regelmatig bijwerken van beleid en procedures:
Beoordeel regelmatig jouw beleid en procedures. Zijn deze nog up-to-date of moeten ze worden aangepast?

Blijf werken aan bewustwording bij medewerkers:
de mens is vaak de zwakste schakel in beveiliging. Houd het onderwerp levend door het thema structureel terug te laten komen, bijvoorbeeld als vast punt op de agenda van iedere teamvergadering.

9 - 12 punten

Een goed begin is het halve werk

Wat betekent dit voor jou?

Je hebt al stappen gezet om je risico's in kaart te brengen, maar er is nog ruimte voor verbetering. Je bent goed bezig, maar er zijn nog enkele gebieden die verdere aandacht vereisen om een hoger niveau van beveiliging te bereiken.

Wat kun je doen om verder te verbeteren?

- Voltooi je risicoanalyse voor alle kritieke processen en systemen. Doe dit samen met de procesverantwoordelijke.
- Breng in kaart welke leveranciers en partners betrokken zijn bij je OT-systemen en beoordeel de risico's die zij met zich meebrengen.
- Train je medewerkers regelmatig in cyber bewustzijn en zorg voor een duidelijk beleid voor het omgaan met kwetsbaarheden.

Praktische tips!

Leveranciers en partners:
Evalueer de cyberbeveiliging van je leveranciers en vraag ze naar hun protocollen en maatregelen.

Medewerkerstraining:
Start met het organiseren van regelmatige trainingen om je OT-medewerkers bewust te maken van de gevaren rondom Industriële cyber beveiliging.

5 - 8 punten

Werk aan de winkel!

Wat betekent dit voor jou?

Je hebt nog niet voldoende inzicht in de risico's van je OT-omgeving. Dit is hét moment om serieus te beginnen met het in kaart brengen van je kwetsbaarheden en het implementeren van de juiste maatregelen om je systemen te beschermen. Maar geen zorgen, het is nooit te laat om te beginnen!

Wat kun je doen om verder te verbeteren?

- Zet een overzicht op van je OT-systemen en de betrokken partijen. (denk aan leveranciers en partners waar jullie aan gekoppeld zijn)
- Voer een grondige risicoanalyse uit voor je kritieke processen.
- Begin met het trainen van je medewerkers op cyberbewustzijn en zorg ervoor dat je externe partners en leveranciers worden gecontroleerd op cyberrisico's.

Praktische tips!

Start met de basis:
Maak een lijst van alle OT-systemen en componenten. Dit is de fundering voor elke risicoanalyse.

In kaart brengen van kwetsbaarheden:
Begin met het onderzoeken van bekende kwetsbaarheden (CVE's) en bepaal welke van toepassing zijn op jouw systemen.

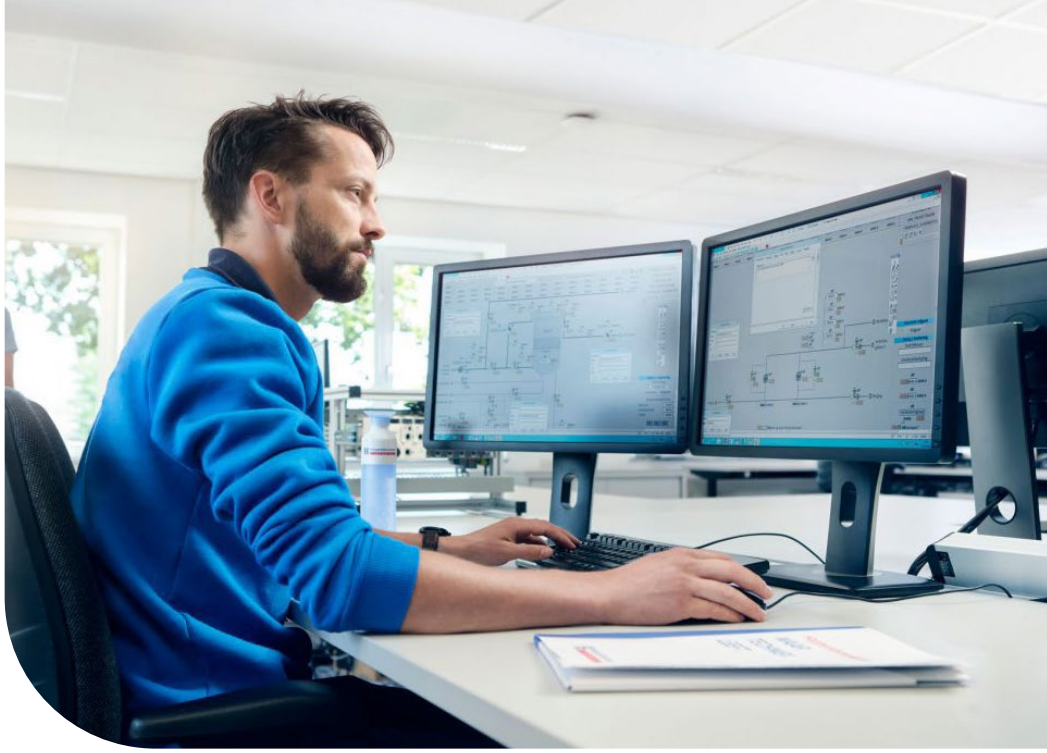
Werk aan bewustwording bij medewerkers: Zorg ervoor dat het onderwerp ook binnen jouw organisatie gaat leven. Meer draagvlak zorgt ervoor dat de kans op succes groter wordt.

Regelmatig bijwerken van beleid en procedures: Beoordeel regelmatig jouw beleid en procedures. Zijn deze nog up-to-date of moeten ze worden aangepast?

Blijf werken aan bewustwording bij medewerkers: de mens is vaak de zwakste schakel in beveiliging. Houd het onderwerp levend door het thema structureel terug te laten komen, bijvoorbeeld als vast punt op de agenda van iedere teamvergadering.

De impact van een Cyberaanval op OT-processen

Een cyberaanval op je OT-omgeving kan ernstige gevolgen hebben. Stel je voor: een aanvaller weet een kwetsbaarheid in je netwerk te benutten en krijgt toegang tot een controlepaneel voor je productielijn. Hierdoor kunnen vitale processen stil komen te liggen, wat leidt tot productieverlies en een vertraagde leveringsketen.



Gevolgen van deze aanval:

- Stilstand van productie: De productielijn komt tot stilstand, wat leidt tot aanzienlijke financiële verliezen en verstoorde klantrelaties.
- Veiligheidsincidenten: De aanvaller zou in staat kunnen zijn om systemen voor veiligheid en monitoring te manipuleren, waardoor de veiligheid van medewerkers en apparatuur in gevaar komt.
- Reputatieschade: Door de verstoring van je OT-processen kan je merk aanzienlijke schade oplopen, vooral als klantbestellingen niet op tijd worden geleverd.

Waarom het belangrijk is om nu te handelen:

Door de risico's nu in kaart te brengen, kun je zulke incidenten voorkomen of minimaliseren. Het creëren van een robuuste OT-omgeving betekent dat je voorbereid bent op bedreigingen en adequaat kunt reageren om je systemen te beschermen.

Zet vandaag nog de volgende stap en versterk je OT-beveiliging!

Het in kaart brengen van je OT-risico's is een cruciale stap in het veiligstellen van je operationele technologie.

Of je nu al goed op weg bent, of net begint, er is altijd ruimte voor verbetering. Gebruik de inzichten uit deze PDF om je OT-omgeving verder te versterken en cyber-dreigingen te minimaliseren.

Meer weten of sparren over jouw situatie?

Onze Industrial Cyber Security-specialisten helpen je graag verder. Of het nu gaat om praktische tips, strategisch advies of een specifieke uitdaging: je kunt altijd vrijblijvend contact met ons opnemen via **ics@hoppenbrouwers.nl.**

hoppenbrouwers

Zet vandaag nog de volgende stap en versterk je OT-beveiliging!

Neem contact op met onze experts voor advies!
Bel 013 – 511 72 27 of klik hieronder.

Mail onze expert >