IT SECURITY ASSESSMENT

IDENTIFICEER DE TECHNISCHE KWETSBAARHEDEN EN RISICO'S

Ontdek de zwakke plekken in uw kantoorautomatisering en/of operationele technologie (OT)-systemen voordat cybercriminelen dat doen! Een IT Security Assessment analyseert uw systemen en biedt handvatten om uw beveiliging te verbeteren en uw organisatie te beschermen tegen bedreigingen die de beschikbaarheid, integriteit en vertrouwelijkheid van uw systemen in gevaar kunnen brengen.

WAAROM EEN IT SECURITY ASSESSMENT?

Een IT Security Assessment is cruciaal voor bedrijven die veel of gevoelige informatie verwerken of waarbij de productie niet stil mag komen te vallen.
Met een IT Security Assessment krijgt u een gedetailleerd overzicht van de kwetsbaarheden in de beveiliging van uw organisatie, zodat u gerichte maatregelen kunt nemen om deze te versterken.

Door uw organisatie te beschermen tegen veranderende cyberdreigingen kunt u met vertrouwen vooruit.

WAT DOEN WE?

BIJ HET UITVOEREN VAN EEN IT SECURITY ASSESSMENT DOORLOPEN WE DE VOLGENDE STAPPEN:

Voorbereiding
Samen bepalen we de scope: welke systemen gaan we controleren op kwetsbaarheden. We kunnen ons bijvoorbeeld richten op de kwetsbaarheid van onlinesystemen (websites, publieke IP-adressen van uw kantooromgeving, inlogmogelijkheden op portalen, Microsoft Azure en Microsoft 365 etc.) of op de kwetsbaarheid van de systemen die zich binnen uw netwerk bevinden. Denk daarbij niet alleen aan pc's, laptops en servers, maar juist ook aan netwerkcomponenten, printers, IP-gebaseerde camerasystemen, telefooncentrales etc.

Alles wat een IP-adres heeft, zich binnen uw netwerk bevindt en reageert op de verzoeken van onze scanners wordt gecontroleerd op kwetsbaarheden. Ten slotte kunt u ook kiezen voor een controle op de kwetsbaarheid van uw industriële systemen (ICS/Scada- of OT-systemen). Natuurlijk kunt u ook kiezen voor alle drie: een maximale controle.

Analyse van geautomatiseerde scans

Nadat de scans, waarbij we controleren op meer dan 200.000 bekende kwetsbaarheden, succesvol zijn afgerond worden de resultaten uit de test(en) geclassificeerd. Een van onze gecertificeerde ethisch hackers – de 'good guys' van het internet - analyseert vervolgens de kwetsbaarheden en classificeert deze met een kritieke, hoge of middelmatige status. De ethisch hacker adviseert u vervolgens over wat u kunt doen om tot verbetering te komen.

Extra controles op locatie

Naast de geautomatiseerde controles kunnen we een ethisch hacker bij u op locatie langs laten komen die extra controles uitvoert.
Denk hierbij aan een juiste beveiliging in de segmentering van uw netwerk, gebruik van wifi, controles op antivirus, controle van de back-up etc.

Rapportages

De kwetsbaarheden die in uw systemen worden gevonden, leggen we vast in heldere, begrijpelijke rapportages. Daarna zullen we deze rapportages met resultaten en aanbevelingen met u en uw IT'er(s) doorspreken. Zo kunnen kwetsbaarheden direct worden weggenomen om uw organisatie beter weerbaar te maken.

DE DRIE GROOTSTE VOORDELEN VAN EEN IT SECURITY ASSESSMENT

Onafhankelijke controle op kwetsbaarheden

Een IT Security Assessment biedt onafhankelijk inzicht in de kwetsbaarheden en risico's van de systemen, applicaties en infrastructuur van uw organisatie. Dit helpt bij het prioriteren van beveiligingsmaatregelen en het minimaliseren van het risico op aanvallen en datalekken.

Expertadvies

Een gecertificeerde ethisch hacker analyseert de bevindingen en geeft heldere terugkoppeling, waarbij eventueel ook interne en externe beheerders kunnen aanschuiven zodat zij de geconstateerde kwetsbaarheden kunnen mitigeren.

Ook controle van OT mogelijk

Ook industriële systemen (ICS/Scada- of OT-systemen) kunnen we opnemen in de IT Security Assessment.