Help, mijn datacenter is gehackt!

KPN Security Services / Han Pieterse

Cyber Security betreft het reduceren van gevaar of schade veroorzaakt door introductie van nieuwe technologie, storing of uitval van ICT of misbruik van ICT tot een aanvaardbaar risico.

Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.

Het reduceren en beheersen van gevaar en/of schade van ICT en het veiligstellen van de identiteit en de continuïteit van de organisatie is het hoofddoel van Cyber Security

KPN Security Services wil transparant zijn over haar aanpak en verwacht hierdoor haar securitybeleid verder te kunnen verbeteren (https://itunes.apple.com/nl/app/kpn-ciso/id1122223795) In de app is het KPN security beleid en een aantal tools beschikbaar gesteld, waarmee security professionals hun eigen beleid kunnen toetsen maar ook de potentiele ernst van kwetsbaarheden en incidenten berekenen.

Agenda

- Hoe veilig is uw Datacenter?
- Hoe kwetsbaar is uw Datacenter?
- Wat kunnen we doen?
- Een PenTest voor uw Datacenter!

Hoe veilig is uw Datacenter?

- Via de bewakingscamera’s zijn hackers het netwerk van het datacenter binnengedrongen en via ‘identity theft’ zijn ze binnengedrongen in het centrale netwerk van de klanten. De dominostenen vallen achtereenvolgens in een niet te keren proces.

Hoe kwetsbaar is uw Datacenter?

- De toegangspoort van uw datacentrum is om ‘onduidelijke’ redenen geblokkeerd. Het hek is dicht en blijft dicht en gelijktijdig staat de brandweer met groot materieel voor de deur vanwege ‘een brandmelding’.

Hoe groot is het risico?

- Binnen het OT domein zijn er wel degelijk cybersecurity risico's, maar ligt de focus vooral nog steeds op de operationele impact. Terwijl aanvallers gebruik maken van zwakheden tussen de ICT en OT infrastructuur, zijn de basics in cybersecurity, goed passwordbeheer, goede authenticatie of patchmanagement, lang niet altijd goed geregeld in het OT-domein.
- Een belangrijk risico is dat industriële host systemen op enigerlei wijze vaak wel verbonden zijn met het internet en via de 'IT-kant' toegankelijk zijn. Volgens schattingen heeft ruim 90 procent van die verbonden systemen een kwetsbaarheid aan boord. In Nederland zou dat neerkomen op bijna 3.000 industriële host systemen met een kwetsbaarheid, waarvan ruim 200 ernstig.
- Verstoringen moeten worden opgemerkt, veranderingen moeten inzichtelijk gemaakt worden en risico's; vanuit welke bron dan ook, moeten afgedekt worden. Maar het is lang niet altijd simpel om op een fysiek zeer moeilijk te bereiken locatie 'even' de nieuwste security maatregelen te nemen of de laatste patches op een embedded system te doen.

Wat kunnen we doen?

- Een eerste stap in de beveiliging van dergelijke kritische infrastructuren is het uitvoeren van een nulmeting en het vaststellen van een goed risicoprofiel, waarbij de ICT omgeving en de OT omgeving **allebei** in kaart gebracht zijn.
- Bij het nemen van security maatregelen kan het datacenter helpen om zoveel als mogelijk de best practises van het NCSC te volgen en de door het NCSC gepubliceerde checklist te gebruiken. https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-publiceert-checklist-beveiliging-ics-scada-systemen.html
- Treffende security maatregelen zijn echter per organisatie verschillend. Voor sommige organisaties zal dat betekenen dat zij systeem hardening in detail zullen moeten toepassen op zowel het ICT als het OT domein. Daarbij worden overbodige functies uitgeschakeld, zal er consequent gepatcht moeten worden en daarnaast gemonitord worden op aanvallen. Voor andere organisaties zal de stap beginnen bij het verhogen van het beveiligingsbewustzijn bij de medewerkers.

Een PenTest voor uw Datacenter!

- Met PenTesting krijgt u inzicht in waar en hoe uw bedrijfsnetwerk of uw operationele netwerk kan worden aangevallen, welke risico’s u daarbij loopt en wat u daartegen kunt doen.
- Met een PenetratieTest onderzoeken experts uw ICT- of OT- infrastructuur op zwakheden en stellen zij vast op welke wijze daar misbruik van gemaakt kan worden. De experts identificeren niet alleen zwakheden, maar gaan nog een stap verder door deze zwakheden ook actief uit te buiten teneinde nog verder door te dringen binnen uw organisatie. Hierdoor krijgt u een duidelijk beeld van eventuele risico’s en acute problemen.
- Ieder Datacenter heeft duizenden IP-nummers in gebruik in uw ICT- en OT- infrastructuur, ook in segmenten van uw infrastructuur waar u het niet zou verwachten. Vele installatie techniek elementen zijn ten behoeve van onderhoud en beheer voorzien van een IP aansluiting. Om zicht te krijgen op de risico’s van de totale complexe infrastructuur van een Datacenter is een PenTest het meest effectieve middel.

Contactgegevens

- Wilhelminakade 123 | P.O.Box 70024| 3000 LE Rotterdam
- Han Pieterse | Senior Solutions Consultant
- Mobile +31 (0)6 23759964
- E-mail han.pieterse@kpn.com
- https://www.kpn.com/zakelijk/blog/is-uw-ot-omgeving-levensgevaarlijk.htm