WORKSHOP RANSOMEWAREAANVALLEN

Het aantal ransomwareaanvallen neemt toe. Organisaties worden vaak verrast door een aanval. In het meest gunstige geval kan een aanval met veel werk worden afgeslagen. In het ergste geval worden gestolen gegevens gepubliceerd. In de gezondheidszorg en overheidsinstellingen heeft publicatie een grote impact op de privacy. M&I/Partners heeft een workshop ontwikkeld die uw organisatie helpt het risico op succesvolle ransomwareaanvallen te verlagen.

Het aantal ransomwareaanvallen neemt schrikbarend toe. Z-Cert.nl houdt op de homepagina zelfs een teller bij van het aantal Europese zorginstellingen dat is besmet met Ransomware. Organisaties worden vaak verrast door een aanval. In het meest gunstige geval kan een aanval met veel werk worden afgeslagen. In het ergste geval ziet een organisatie zich gedwongen de cybercriminelen te betalen. Niet alleen voor het vrijgeven van de encryptiesleutel, maar ook om te voorkomen dat gestolen gegevens worden gepubliceerd. In de gezondheidszorg, het onderwijs en bij overheidsinstellingen heeft publicatie een grote impact op de privacy.

Workshop ransomwareaanvallen

Simpelweg implementeren van lijstjes met maatregelen helpen onvoldoende om ransomwareaanvallen aan te pakken. Voor Ransomware-aanvallen geldt: hoe meer risico's worden aangepakt hoe kleiner de blootstelling van de organisatie aan ransomware. **M&I/Partners heeft een workshop ontwikkeld die uw organisatie helpt het risico op succesvolle ransomwareaanvallen te verlagen.**

Resultaat

Een beknopte overzicht van de grootste risico's inclusief advies en aanbevelingen om de risico's te verminderen. Het is ook mogelijk een technisch onderzoek te doen naar kwetsbaarheden binnen de IT-infrastructuur.

M&I/Partners/

Workshop Ransomwareaanvallen

De workshop en risicoaanpak van M&I/Partners is gebaseerd op jarenlange ervaring en de gepubliceerde lessons learned bij bekende aanvallen (Hof van Twente en de Universiteit Maastricht). Wij kijken naar de organisatie van de opdrachtgever en de toegepaste maatregelen om ransomwarebesmetting te voorkomen of om te herstellen van een ransomwareaanval.

In de workshop nemen wij betrokken medewerkers mee in belangrijke praktijkrisico's. Daarbij bespreken we welke maatregelen de organisatie heeft genomen om de risico's aan te pakken. Voor risico's die onvoldoende zijn afgedekt wordt een actielijst vastgesteld. In de workshop verkennen we samen de risico's op besmetting met ransomware op het gebied van:

- awareness van personeel;
- maatregelen om het aanvalsoppervlak te beperkten;
- middelen om ransomware op te sporen;
- monitoring;
- controle van de last line of defense;
- ransomware scenario's.

De workshop is als volgt opgebouwd

1. Verkenning bestaande maatregelen om ransomware tegen te gaan binnen de organisatie.
2. Verkenning van de back-up als "last line of defense" binnen de organisatie.
3. Uitvoering van de risicoanalyse.

Deelnemers workshop

Deelnemers aan de workshop bestaan bijvoorbeeld uit een Netwerkbeheerder, Back-up beheerder, Operationeel IT-manager en Security Officer.

Meer weten?

Wilt u deze workshop inzetten in uw eigen organisatie, meer weten over aan workshop of vrijblijvend sparren over ransomwareaanvallen? Neem contact op met Victor Meerloo

- victor.meerloo@mxi.nl
- 06 82 36 38 93