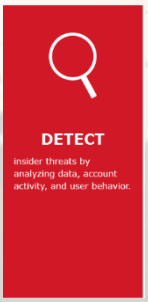
IO4U Operationeel Plan

Onze dienstverlening is gebaseerd op een operationeel plan met een vaste structuur en aanpak. Dit document geeft u een omschrijving van deze aanpak. Onze aanpak bestaat uit 3 fasen, te weten Detect, Prevent en Sustain.

Deze fasen kunnen naargelang de beschikbare resources (tijd, geld en middelen) worden aangepast. In overleg zullen wij de doorlooptijd bepalen maar ook de activiteiten. Met name in de tweede fase zullen wij meer gaan verlangen van uw interne organisatie. De eerste fase bestaat voornamelijk uit het in kaart brengen van de risico's, prioriteiten en activiteiten.

DETECT (FASE 1)

Binnen de fase “Detect” zullen wij door het analyseren van de Active Directory en het file systeem de urgente en belangrijkste risico’s in kaart brengen. Deze fase wordt afgesloten met een presentatie waarin de bevindingen worden gepresenteerd alle stakeholders. Onze bevindingen zullen wij onderbouwen met een BowTie. In de praktijk is er een afvaardiging van Directie/management, IT, Security en Compliance aanwezig bij deze presentatie.



Analyse Active Directory

1. Welke personen\groepen\afdelingen hebben toegang tot welke files\folders\shares\bestanden?
2. Bepalen wie de owner van files\folders\shares zou kunnen zijn op basis van het gebruik van deze files\folders\shares
3. Wie heeft welke files\folders aangemaakt\gewijzigd en wanneer, en wat\in welke mate aangepast?
4. Hoe zijn de rechten op specifieke files\folders\shares in de loop der tijd gewijzigd?
5. Hoe is de samenstelling van de groep(en)/afdeling met rechten op bepaalde files\folders\shares in de loop van de tijd gewijzigd.
6. Wie hebben een specifiek bestand verwijdert\geopend\gekopieerd?
7. Zijn er gebruikers die veel bestanden kopiëren (mogelijk meenemen bestanden bij ontslag)?
8. Zijn er gebruikers die in korte tijd veel bestanden aanpassen (cryptolocker)?
9. Archief data inzichtelijk maken (Omvang, locatie en gebruik).

Binnen deze fase worden bijvoorbeeld ook de volgende zaken in kaart gebracht.

1. Wie heeft toegangsrechten aangepast op een bestand\folder?
2. Classificatie en discovery van gevoelige data (paspoorten, BSN, persoonsinformatie, bankrekeningnummers, contracten, intellectuele eigendommen, ...)
3. Monitoring en alerting op verdacht gedrag (User Behaviour & predefined rules)
4. Alerting op verdachte handelingen, signalering en actie o.b.v Powershell script.
5. Wie heeft welk document gedeeld en met wie (Specifiek Sharepoint / incl. externe sharing) en het gedrag van de gebruikers de bedreigingen en kwetsbaarheden gaan identificeren.

PREVENT (FASE 2)

Deze fase bevat het opnieuw structureren van de rechten, het beveiligen van “exposed data” en vaststellen en betrekken van dataeigenaren. Deze fase elimineert de “High Risk” problemen, beperkt de omvang van een beveiligingsissue, vereenvoudigd de omgeving en betrekt de stakeholders buiten IT/Security. De volgende stappen zullen wij in deze fase doorlopen.

KPI’s bepalen

In deze fase zullen wij de KPI’s gaan vastleggen om het management te kunnen informeren over de voortgang. Door een baseline op te stellen kunnen we wekelijks, maandelijks of iedere andere periode het management informeren over de voortgang. Samen met uw organisatie zullen we de relevante KPI’s opstellen.

Beveilig gevoelige data en beperk toegang tot archief data

Zorg ervoor dat de toegang tot gevoelige of gereguleerde data tot een minimum wordt beperkt. Deze data kan, eenmaal geïdentificeerd, in quarantaine worden geplaatst, verwijderd of worden versleuteld.

Repareer AD en file system problemen

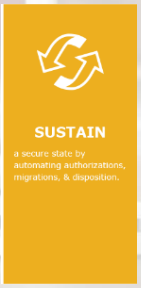
Elimineer onnodige en in potentie gevaarlijke onderdelen binnen het file system en Active Directory. Aanvallers gedijen het beste bij chaos en complexiteit. Complexe omgevingen verhogen de kans op een aanval maar maken de verdediging ook een stuk moeilijker.

Verder zullen de volgende stappen moeten worden genomen;

- Elimineer globale groepen
- Vereenvoudig rechten en toegang
- Verwijder onnodige rechten
- Identificeer data eigenaren

SUSTAIN (FASE 3)

Deze fase behelst het werken en onderhouden van de “nieuwe structuur”. Hiermee bedoelen we dat de opgeschoonde omgeving, die ontdaan is van de risico’s, samen met data eigenaren op een slimme efficiënte manier wordt gebruikt en onderhouden.



Niet alle omgevingen zijn hetzelfde, echter onze ervaring leert dat de volgende onderdelen bij veel organisaties in fase 3 vaak voor komen:

Monitoring van gebruikers en datagebruik (audit trail)

Door continue te blijven monitoren behouden we de baseline van gebruik, waardoor we snel kunnen optreden als er een incident is. Tevens is deze audit trail de basis om te bepalen welke data wordt gebruikt. Dit is dan weer input voor regulaties waar een meld-, bewaar- of vernietigingsplicht onderdeel van is.

Real time alerting

Automatische alerting op afwijkingen van het normale gedrag van gebruikers en andere accounts. Nieuwe bedreigingen die om welke redenen dan ook toch langs de firewall en andere security oplossingen heen komen zullen deze triggers veelal laten afgaan waardoor de impact tot een minimum en vaak zelfs tot nul beperkt kan worden.

Automatische verplaatsing van data

Doordat we nu volledig in control zijn over de ongestructureerde data, kunnen we met behulp van wat extra tools deze data ook automatisch gaan verplaatsen. Hierdoor zorgen we voor een schone omgeving die ook nog eens compliant is. Het verplaatsen kan diverse doeleinden hebben, zoals:

- GDPR compliancy
- Wetgevingen waar een meld-, bewaar- of vernietigingsplicht in beschreven is.
- ISO certificeren, NEN normeringen
- Archiveringsbeleid
- Bescherming van intellectueel eigendom

Automatische workflows t.b.v. berechtingen

De dataeigenaren dienen in de nieuwe structuur rechten goed te keuren en entitlement reviews te doen over de dataset waar zij verantwoordelijk voor zijn. Een systeem waarin men dit geautomatiseerd kan doen maakt dit werk makkelijker, minder foutgevoelig en beter te managen. Ook het automatisch intrekken van rechten kan een dergelijk systeem in voorzien.

Wilt u meer weten?

Voor informatie kunt u direct contact opnemen met uw contactpersoon. Indien u nog geen contactpersoon heeft zijn wij te bereiken op het onderstaande algemene telefoonnummer. U kunt ons uiteraard ook een e-mail sturen en/of onze website raadplegen.

IO4U BV

www.io4u.nl
info@io4u.nl
085 90 20 470