BECHTLE'S

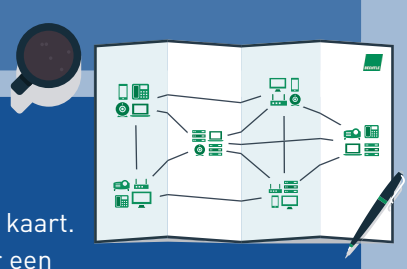
IT-securityladder

Cybercriminelen worden steeds slimmer en het aantal beveiligingsincidenten stijgt. In 2021 zijn er maar liefst 5,1 miljard datarecords gelekt door cyberaanvallen, ransomware en interne fouten. Dat is een flinke stijging van 11% ten opzichte van 2020. Security blijft voor veel organisaties dus een uitdaging. Het beschermen van bedrijfsgegevens staat gelukkig wel steeds hoger op de agenda. Bij Bechtle hebben we de IT-securityladder ontwikkeld om je op weg te helpen.

Welke stappen moet je zetten om jouw organisatie zo goed mogelijk te beschermen?

0

Information Security Framework
Dit is het ideale startpunt voor ieder securitytraject. Deze stap richt zich vooral op 'mens & organisatie' en nog niet op je IT-infrastructuur. Het Information Security Framework is een gestructureerde en toegankelijke methode om samen met jouw organisatie de situatie rondom informatieveiligheid in kaart te brengen, keuzes te maken over de aanpak en de maatregelen duurzaam te implementeren.

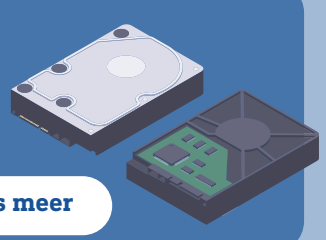


1

Bechtle Inventory Services
Met de Bechtle Inventory Services brengen we je volledige IT-omgeving in kaart. Wij zijn van mening dat dit de basis is van waaruit je moet vertrekken voor een sterk securitybeleid.

2

Backup & recovery
Back-up is belangrijk, in het bijzonder als je slachtoffer wordt van een ransomware-aanval. We merken helaas nog steeds dat organisaties in de veronderstelling zijn dat er een back-up beschikbaar is, maar deze na een calamiteit niet teruggezet kan worden.



Lees meer

3

Network security
Het doel is om een ononderbroken netwerkbeschikbaarheid en een robuuste toegang tot je bedrijfsnetwerk en applicaties te creëren.

Lees meer

4

Endpoint security
Desktops, laptops en smartphones worden extra beschermd. Maar denk ook aan het toenemende aantal sensoren, printers en auto's die via het internet verbinding maken met het bedrijfsnetwerk.

Lees meer

5

E-mail security
Omvat een scala aan procedures en technieken om ervoor te zorgen dat je medewerkers veilig kunnen mailen. Tools voor e-mailbeveiliging helpen om het grootste deel van onbetrouwbare mails te identificeren en te blokkeren voordat ze bij jouw collega's terechtkomen.

Lees meer

6

Multifactor Authentication
Gestolen identiteiten zijn de grootste oorzaak van datalekken. Vraag daarom als extra controle met MFA naar specifieke informatie die alleen de eindgebruiker weet, of door te controleren via biometrische- of locatiegegevens.

7

Network Access Control
Dankzij NAC krijgen alleen geverifieerde gebruikers en apparaten die zijn geautoriseerd en voldoen aan jouw securitybeleid, toegang.

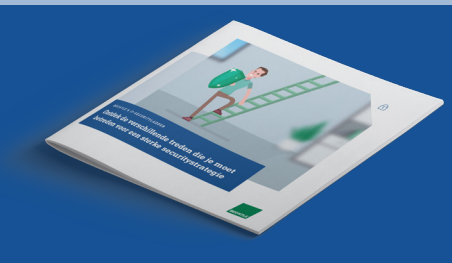
8

Security Information and Event Management
Logging en reporting is enorm belangrijk. Het kan je helpen om proactief technische problemen op te lossen, maar ook bijdragen aan auditing, monitoring en incident response.

9

Data Lifecycle Management
DLP toepassingen helpen om je gevoelige informatie te detecteren, classificeren en beveiligen. waar deze zich ook bevindt of naar onderweg is. Deze toepassingen hebben als doel om patronen in jouw gegevens te ontdekken, je gegevens te beschermen en dataloss te voorkomen.

Wil je meer weten over de securityladder? Lees dan gratis de whitepaper 'Ontdek de verschillende treden van de securityladder voor een sterke securitystrategie' of neem contact op met onze specialist. Hij staat je graag te woord met advies.



Download de whitepaper

Patrick Voss
Solution advisor security
T +31 40 760 2915
patrick.voss@bechtle.com

BECHTLE