WHITEPAPER

Cyber Resilience Assessment

avit

part of springboardnetwork

ONTDEK DE STAAT VAN JOUW SECURITY

Het aantal security-incidenten neemt toe en de effecten zijn duidelijk zichtbaar. Sommige incidenten veroorzaken kort 'ongemak' (DDOS), maar sommige zorgen ervoor dat essentiële bedrijfsprocessen worden onderbroken of leiden tot problemen in het publieke domein (zoals ransomware).

Door recente gebeurtenissen en voorspellingen staat dit onderwerp bovenaan de agenda van veel organisaties. Onze Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC) adviseren om voor te bereiden op een groeiend aantal cyber-dreigingen. Dat sluit aan bij de trends voor 2023.

Om de dreiging in cijfers uit te drukken: de economische schade van cybercrime voor 2021 wordt geschat op 10 miljoen euro voor Nederland. De wereldwijde cybercrime-economie in 2021 zou zes triljoen dollar bedragen, waarmee het de derde economie van de wereld is.

Krijg grip op deze dreigingen met het Avit Cyber Resilience Assessment, dat jouw huidige staat van security weergeeft. Met de resultaten beslis je of je actie onderneemt, of dat je acceptabele risico's voor lief neemt.

"Om de dreiging in cijfers uit te drukken: de economische schade van cybercrime voor 2021 wordt geschat op 10 miljoen euro voor Nederland."

WAAROM HET CYBER RESILIENCE ASSESSMENT?

Het Cyber Resilience Assessment ondersteunt jouw organisatie door de IT-omgeving te beoordelen op veelvoorkomende en belangrijke, real-world cyberdreigingen. Daarbij worden minimaal vijftien onderwerpen onder de loep genomen.

Dit assessment focust niet alleen op IT asset management, maar beoordeelt ook veiligheids-gerelateerde procedures, maatregelen, en de menselijke factor (zoals training en bewustzijn).

Ons rapport bestaat uit aanbevelingen om security-dreigingen sneller te ontdekken en af te dekken. Om jouw organisatie te beschermen én om beter te reageren bij incidenten.

Na het assessment nemen onze security-experts je mee door de resultaten, bespreken we samen de uitkomst van elk onderwerp, en krijg je betekenisvol advies. Gebruik dit advies om risico's te accepteren of de effectiviteit van nieuwe security-maatregelen te voorspellen. Zo voorkom je dat businesscontinuïteit in gevaar komt.

Voorwaarden Cyber Resilience Assessment

Het Cyber Resilience Assessment bestaat uit interviews met een kleine groep medewerkers (vertegenwoordigers) binnen de IT-organisatie. De beschikbaarheid van deze vertegenwoordigers is daarom een randvoorwaarde. Normaal gesproken bestaat deze groep van mensen uit:

	Vereist	Optioneel
Network engineer	x	
System engineer	x	
Support engineer	x	
Security officer	x	
IT Progress manager		x
CIO		x

Dit assessment heeft als doel om de huidige staat van security te ontdekken. Alle positieve (of minder positieve) resultaten worden weergegeven in een visuele grafiek. De resultaten zijn niet bedoeld om medewerkers te bekritiseren, maar geven de huidige security-staat weer. We verwachten daarom dat het meewerkend personeel de vragen eerlijk beantwoordt (zelfs als het steekt), om alle gewenste informatie te kunnen verzamelen.

Avit behandelt de ontvangen informatie en vergaarde inzichten vertrouwelijk. Alle informatie blijft binnen de organisatie en bij de CX-teams die aan de opdracht werken.

Om dit assessment toegankelijk te houden worden alle antwoorden van medewerkers als de waarheid aangenomen. Een third-party assessment (bijvoorbeeld met bewijs van onze security-experts) of een uitgebreider assessment, kunnen we op maat ontwikkelen.

WAT WE DOEN

Alle activiteiten zijn verdeeld in drie fases:

1. We interviewen de vertegenwoordigers, bij voorkeur op locatie. In twee tot vier uur stellen we de staat van security vast op basis van vijftien verschillende security-onderwerpen. Onze security-expert maakt hier een rapport uit op, waarin visuals de security-staat van jouw organisatie weergeven.

2. Onze security-expert bespreekt het assessment met jouw security-team. Zo geven we actiegericht advies op maat, naast de inzichten uit het rapport. Het volledige rapport bestaat uit een algemeen overzicht, quick wins en advies tot verbetering op cruciale onderwerpen.

3. We loodsen je uiteindelijk door het document, om zeker te weten dat het assessment door alle betrokkenen wordt begrepen. Deze 'walkthrough' maakt het ook mogelijk om direct vragen te stellen aan onze specialist. We voeren een herziening door voor we het definitieve rapport overhandigen.

Follow-up assessment

Naast het assessment kan Avit ook de publieke staat van security beoordelen op basis van 20 verschillende onderwerpen. Dit follow-up-assessment is gebaseerd op publieke informatie die hackers gebruiken om te berekenen hoeveel kans van slagen een aanval heeft. Voor alle gevonden problemen krijg je gestandaardiseerde suggesties voor passende acties. Onze security-experts nemen het rapport bovendien met je door voor advies op maat.

Saleguard	Privacy	Resiliency	Reputation
i Digital Footprint	B SSL/TLS Strength	A Attack Surface	i Brand Monitoring
A Patch Management	A Credential Mgmt.	A DNS Health	A IP Reputation
A Application Security	A Hacktivist Shares	A E-mail Security	A Fraudent Apps
A CDN Security	A Social Network	A DDoS Resiliency	A Fraudent Domains
A Website Security	C Information Disclosure	A Network Security	A Web Ranking

DOORLOOPTIJD EN DELIVERABLES

Het assessment heeft normaal gesproken een doorlooptijd van twee dagen, met een korte evaluatie op dag drie. De activiteiten kunnen niet direct na elkaar worden uitgevoerd en zijn daarom verdeeld over een paar dagen. De activiteiten voor jouw organisatie beperken zich tot een security assessment workshop die de eerste helft van dag één in beslag neemt, en een 'walkthrough' door de resultaten op dag twee.

SECURITY ASSESSMENT WORKSHOP

Dagdeel 1

Security assessment workshop
- Setting the scene
- Kennismaking team
- Assessment uitvoeren

Security assessment workshop

Dagdeel 2

Resultaten doorlopen
- Algehele staat van security bespreken
- Alle onderwerpen doorlopen
- Alle kansen tot verbetering bespreken
- Algemene discussie

Walkthrough of the results

Dagdeel 3

Evaluatie
- Evaluatie uitgevoerd door CSM of AM
- Resultaten van evaluatie bespreken
- Bespreken andere behoeftes
- Algemene discussie

Evaluation

Dagdeel 4

Rapport maken
- Rapport wordt gecreëerd met actiegerichte visuals

Creating the report

Dagdeel 5

Definitief rapport maken
- Laatste inzichten doorvoeren
- Rapport finaliseren
- Rapport naar alle sleutel-betrokkenen sturen

Creating of the final report

VOORDELEN CYBER RESILIENCE ASSESSMENT

Het Cyber Resilience Assessment geeft een snel en helder overzicht van de IT security-staat van een organisatie. Daardoor heeft iedereen dezelfde informatie en aanbevelingen voorhanden. Op die manier kan de organisatie risico's afwegen, en beslissen of deze geaccepteerd of aangepakt worden.

Door het assessment krijgt een CIO of CSO een plan voor security-verbeteringen, gerangschikt op prioriteiten en impact. Geprioriteerde acties kunnen meegenomen worden naar de raad van bestuur, om gemakkelijker budget veilig te stellen. Een CFO krijgt dankzij het assessment inzicht in de prioriteiten en kosten van een aangepaste security-strategie. Zo kunnen waardevolle investeringen gepland worden om het security-niveau van de organisatie te verbeteren.

GEÏNTERESSEERD IN EEN ASSESSMENT?

Vraag het Cyber Resilience Assessment nu aan, of neem vrijblijvend contact met ons op.

Onze security-specialisten beantwoorden jouw vragen graag.

avit
part of springboardnetwork

T: +31 (0)88 032 10 32
E: info@avitgroup.com