TEAM ROCKSTARS IT

IT SECURITY SCAN

JOUW CYBERSECURITY ON POINT

JOUW **CYBERSECURITY ON POINT** MET DE TEAM ROCKSTARS IT SECURITY SCAN

Cybersecurity is een hot topic. Cyberaanvallen bij grote bedrijven als Uber en T-Mobile lijken aan de orde van de dag, en de inzet van malware om het elektriciteitsnet van Oekraïne plat te leggen zit ons vers in het geheugen. Een onderzoek van IBM* schat de gemiddelde kosten van een cyberaanval in op 4.4 miljoen euro. Reden genoeg om te zorgen dat jouw cybersecurity 'on point' is. Daar komt bij dat er steeds meer wet- en regelgeving komt op het gebied van informatie-beveiliging, ook voor bedrijven die daar eerder nog niets mee van doen hadden.

Om te weten waar jouw bedrijf staat op het gebied van informatiebeveiliging en cybersecurity is het verstandig om een Security Scan uit te voeren. Met de resultaten van deze Security Scan worden risico's en verbeterpunten blootgelegd. Daarnaast kan het regelmatig herhalen van de Security Scan ook progressie of verslechtering aantonen. Het is daarmee een ideale tool om jouw bedrijf klaar te maken voor de toekomst. Waarom je natuurlijk kiest voor een Team Rockstars IT Security Scan, dát lees je in dit document.

WETEN WAAR JE STAAT MET EEN SECURITY SCAN

Een Security Scan geeft inzicht in jouw specifieke IT-situatie ten opzichte van industrie standaarden. Na zo'n scan weet je precies waar jouw risico's en verbeterpunten zitten en kun je een plan maken om deze aan te pakken. Een Security Scan uit laten voeren is altijd waardevol; proactief om een benchmark te krijgen, of reactief op basis van een bepaalde trigger.

PROACTIEF SCANNEN

Voorkomen is beter dan genezen. Je weet immers niet wat je niet weet. Mogelijke risico's die uit een Security Scan kunnen komen zijn:

- Er is geen of onvoldoende zicht op de infrastructuur waardoor malware zich eenvoudig kan verspreiden
- Er is geen response en recovery plan aanwezig waardoor het lang duurt om te herstellen van een mogelijke aanval
- De Cybersecurity Policy is (onvoldoende) bekend bij medewerkers
- Data wordt niet of onvoldoende versleuteld

REACTIEF SCANNEN

Soms ontvang je triggers die een directe aanleiding zijn om een Security Scan uit te laten voeren. Je kunt dan denken aan:

- Wijzigingen in wet- en regelgeving, waardoor jouw business te maken krijgt met bepaalde (nieuwe) compliance eisen
- Berichten in het nieuws over een grote cyberaanval binnen jouw sector, waardoor het risico voor jouw business heel dichtbij komt
- Emails of andere phishing technieken die worden gemeld door jouw klanten of werknemers

MOET MIJN IT HIERVOOR AL IN "DE CLOUD" ZITTEN?

Nee, het maakt niet uit of je je IT-landschap en daarmee mogelijk ook digitale dienstverlening (deels) ingericht hebt in een (publieke) cloud omgeving of niet. Een Team Rockstars IT Security Scan kijkt vooral naar processen. Dat kunnen zowel processen zijn die zijn ingericht rondom een cloud of on-prem omgeving.

WAAROM DE TEAM ROCKSTARS IT SECURITY SCAN?

Een Team Rockstars IT Security Scan is bedoeld om op proces niveau te kijken naar de informatiebeveiliging van jouw bedrijf, afdeling of product. Dat maakt de Rockstars Security Scan significant anders dan bijvoorbeeld een pentest. Met een pentest worden alleen problemen in de implementatie van applicaties vastgesteld. Een Team Rockstars IT Security Scan geeft een breed inzicht in de informatiebeveiliging: hoe zijn jouw processen ingericht op het gebied van security. Onze Security Scan is ook geen audit. Er komen risico's naar boven uit onze scan, maar het is vervolgens aan jou als klant om te bepalen of en wat daar de implicaties van zijn.

Daarnaast zijn er nog een aantal andere redenen waarom onze Security Scan de beste keuze is:

- Team Rockstars IT brengt alle expertise mee om de ontwikkelingen in- en de complexiteit van de cybersecurity te begrijpen. Wij volgen de industrie en de wetgeving op de voet en delen onze kennis graag met jou
- Team Rockstars IT leidt je volledig door het proces van de scan en legt de uitkomsten in begrijpbare taal uit
- Aan de hand van de scan worden onafhankelijke conclusies getrokken die helemaal zijn toegespitst op datgene wat voor jou belangrijk is
- Een Security Scan kent een aantal standaard checks. In overleg met jou kunnen we daarnaast extra focus leggen op bepaalde onderdelen of bepaalde specifieke vragen beantwoorden
- Bij Team Rockstars IT zijn we pas tevreden als jij je gewenste target hebt behaald en je je helemaal zeker voelt over jouw informatiebeveiliging

DE SECURITY SCAN IN ZES HELDERE STAPPEN

Hebben we je overtuigd? Dan gaan we aan de slag!

1. INTAKE & SCOPING

Tijdens het eerste gesprek met jouw Lead Consultant is het belangrijk om de scope van de Security Scan te bepalen. Dit om te voorkomen dat er componenten niet binnen de scan vallen waarvan de klant dit wel verwacht, of dat er onnodig veel tijd gestoken wordt in het beoordelen van componenten die niet beoordeeld hadden hoeven worden. De scope kan bijvoorbeeld één softwareproduct of service zijn, of het primaire bedrijfsproces met de daarbij ondersteunende IT-componenten.

Team Rockstars IT werkt met een standaard framework voor de Security Scan. Dit framework bestaat uit een set maatregelen die bedrijven en instellingen helpen om zich weerbaarder te maken tegen cyberaanvallen. Samen stellen we een target, zodat we weten waar jij als klant uiteindelijk wil staan als het gaat over informatiebeveiliging.

2. INTERVIEWS

Alle componenten die in de scope van het project zitten worden beoordeeld in de Security Scan. De score van een bepaald component wordt vastgesteld door middel van interviews met stakeholders binnen jouw bedrijf.

3. SCORING & RISICO'S

Op basis van de interviews maken we de huidige stand van zaken binnen jouw organisatie meetbaar en inzichtelijk. Dat doen we door het toekennen aan scores aan alle individuele componenten. Naast inzicht in de huidige status geven de scores je ook inzicht in de route die nog voor je ligt om uiteindelijk het target-level dat we hebben bepaald te halen.

Naar aanleiding van de behaalde scores per component stellen we vast wat de risico's zijn. Deze risico's zijn geen standaard antwoorden, maar worden specifiek voor jouw situatie beschreven.

4. FEEDBACKSESSIES

Na het bepalen van de scores en de bijbehorende risico's wordt er teruggekoppeld aan de geïnterviewde personen. Eventuele misverstanden worden hiermee weggenomen en het versterkt het gevoel van een open dialoog. Bovendien voorkomt het verrassingen bij de oplevering van het eindrapport.

5. RISK LOG & RISICO SCENARIO'S

Een risk log geeft inzicht in alle gevonden risico's. Deze zijn opgebouwd uit een combinatie van de risico's van de individuele componenten. Daarbij wordt ook de mate van het risico ingeschat.

De risico's die in het risk log staan zijn vaak vrij technisch van aard. Daarom maken wij ook risico scenario's, zodat de risico's ook voor mensen zonder technische achtergrond volkomen duidelijk zijn.

6. HET EINDRAPPORT

Het eindrapport dat je na de Security Scan ontvangt laat zien hoe het onderdeel waarop de scan is uitgevoerd ervoor staat. Het geeft een overzicht van de risico's die er in het proces zijn en hoe die risico's samen concrete bedreigingen naar de bedrijfsvoering vormen. In het eindrapport staan ook verschillende component rapporten; de leesbare versie van de resultaten van de interviews. Het volledige eindrapport is te vertalen naar concrete verbeterpunten en helpt om prioriteiten te stellen. Bovendien bevat het een aantal aanbevelingen over hoe het gewenste target niveau te gaan behalen.

SAMEN OP REIS NAAR EEN OPTIMALE BEVEILIGING VOOR JOUW BEDRIJF

Met de inzichten die de Security Scan oplevert kunnen we samen concrete acties definiëren waarmee je naar een optimale inrichting van jouw informatiebeveiliging kunt toewerken. Wij kunnen je helpen bij het bepalen van de prioriteiten en het opstellen van een verbeterplan. Dat kan bijvoorbeeld een roadmap zijn met aanpassingen en veranderingen voor de korte en lange termijn, om uiteindelijk een ISO27001 certificering te behalen. Team Rockstars IT kan je hier natuurlijk in ondersteunen. Wij hebben de juiste mensen in huis om jou verder te helpen. Bijvoorbeeld in de vorm van:

- Security Engineers die je ontwikkelproces veiliger kunnen maken
- Architectuur Specialisten die de kern van je architectuur onder de loep kunnen nemen

Of we brengen je in contact met een specifieke Security Specialist die voor jouw casus nodig is, ook als we deze niet in huis hebben.

Wij gaan graag samen met jou op weg naar een optimale beveiliging van je bedrijf. Zodat jij je weer met een gerust hart kunt bezighouden met datgene waar jij energie van krijgt.