KPMG

100% IT-veiligheid bestaat niet

Maximale voorbereiding wel

100% IT-veiligheid bestaat niet, maximale voorbereiding wel

Vaak hebben burgers geen keus als het gaat om welke gegevens ze moeten delen met de overheid en op welke manier. Je zou kunnen zeggen dat het hun recht is om dat op een veilige manier te kunnen doen. Gelukkig hebben overheden veel manieren om hun (digitale) weerbaarheid te verhogen. En hoewel de overheid en hun IT-systemen niet altijd synoniem staan voor succes, zijn er zeker succesverhalen te vinden. Een bekend voorbeeld is DigiD: al in 2003 geïntroduceerd en inmiddels niet meer weg te denken. Het is bovendien een goede eerste les: vaak wordt gedacht dat beveiligingsmaatregelen de ontwikkelsnelheid beperken of de gebruikerservaring negatief beïnvloeden. Maar juist DigiD maakt het voor burgers makkelijker zich te identificeren. Ontwikkelaars kunnen op hun beurt vertrouwen op de DigiD-documentatie en hoeven niet zelf het 'security-wiel' uit te vinden.

De belangrijkste aspecten voor veiligheid

Het is belangrijk om te weten dat 100% veiligheid niet bestaat en dus ook nooit gegarandeerd kan worden. Zelfs niet vanuit de overheid. Wat wél kan is de veiligheid maximaal borgen. Daarbij speelt een aantal zaken een belangrijke rol:

01 **Bepaal het dreigingslandschap en het aanvalsoppervlak.** Welke hackers zouden geïnteresseerd zijn in de data? Gaat het om boze burgers, criminelen, of andere landen? Dat maakt nogal uit voor de mate van dreiging. Bedenk vervolgens op welke manieren ze kunnen aanvallen. Via internetservers? Via medewerkers? Door phishing of afpersing?

02 **Neem al bij het inrichten van processen en systemen security mee.** Achteraf pas bedenken hoe iets beveiligd moet worden is lastiger, duurder en vaak minder veilig.

03 Omdat je er altijd van uit moet gaan dat een hack zou kunnen plaatsvinden, is het belangrijk **beveiliging in verschillende lagen te ontwerpen**. Zelfs als er een inbraak is, heeft de hacker niet meteen toegang tot alle data.

04 Heel belangrijk: **creëer mechanismen die zorgen dat je weet dat er een aanval plaatsvindt of dat er misbruik wordt gemaakt.** Hoe eerder je in de gaten hebt dat er een aanval is, hoe sneller je immers passende maatregelen kunt nemen.

05 De vervolgstap is **heldere processen inrichten zodat er goed gereageerd wordt.** Denk aan het isoleren van systemen of het naar buiten werken van de aanvallers.

06 Ten slotte, **zorg dat je oplossingen inricht voor het herstellen van je digitale omgeving**, bijvoorbeeld door het consequent bijhouden van back-ups.

De BIO-baselijn als basis voor veiligheid

Er zijn veel raamwerken waarop overheden kunnen steunen als het gaat om securitymaatregelen. Sinds 2019 is de Baseline Informatiebeveiliging Overheid (BIO) verplicht. Het gaat om een uniform normenkader op verschillende niveaus en is daarmee breed toepasbaar voor allerlei verschillende overheids-diensten. BIO wordt bijgehouden en geüpdatet, zo komt vanaf eind 2024 BIO2.0 beschikbaar. Ook hierbij geldt: het is niet automatisch een garantie voor een veilige of zelfs weerbare organisatie, het is slechts de start. Voldoen aan de normen is wat anders dan daadwerkelijk veilig zijn. Dat komt voor een groot deel omdat veiligheid simpelweg te complex is om binnen een normenkader te vatten, het is nooit compleet. BIO is niets meer dan een baselijn – waarna het echte werk begint.

Testen, testen en testen

Om te weten of je naast compliant ook echt weerbaar bent, is regelmatig testen essentieel. Een beetje vergelijkbaar met een brandoefening. Het gaat om meer dan de juiste brandmelders op de juiste plekken. Het gaat er ook om of de mensen niet toch de lift pakken als het alarm gaat. Zo'n oefening noemen we (cyber)aanvalssimulaties of Red Teaming. Speciaal voor dit soort oefeningen heeft de overheid in 2023 twee nieuwe raamwerken gelanceerd: Threat Intelligence Based Ethical Red Teaming (TIBER) en Advanced Red Teaming (ART). Daarnaast is er een Gereedschapskist Red Teaming en een keuzehulp beschikbaar.

Een realistisch uitgevoerde aanval

Tijdens dit soort oefeningen worden professionele ethische hackers ingehuurd (de zogenaamde Red Teamers) die realistische cyberaanvallers simuleren. Ze kunnen dat vanuit verschillende rollen doen, van activisten tot georganiseerde criminaliteit. Uiteraard is het belangrijk dat intern slechts een selecte groep mensen weet dát er een oefening plaatsvindt. Alleen zo kan de 'echte' reactie worden gemeten. Het team dat op de hoogte is, heet het White Team of het Control Team. De aanval zelf volgt altijd een vooraf opgesteld scenario waarbij op basis van (semi)openbare bronnen wordt vastgesteld welke (potentieel gevoelige) informatie kan worden gestolen. Het vastgestelde patroon zorgt ervoor dat het White Team weet wat het kan verwachten én in de gaten kan houden of eventuele detecties horen bij de simulatie of dat er onverhoopt een echte aanval plaatsvindt. Zo'n aanval kan allerlei vormen krijgen, van phishing bij werk-nemers via LinkedIn tot het uitbuiten van een kwetsbare website. Eenmaal binnen, wordt er gekeken hoe er van systeem naar systeem gesprongen kan worden. Alles met het vooraf bedachte einddoel in zicht.

En dan: wat kan er beter?

Na afloop gaan de betrokkenen rond de tafel zitten. Wat is er goed gegaan en wat heeft de organisatie gemist van de aanval? Zo kunnen verbeterpunten worden vastgesteld. Vaak wordt de aanval letterlijk nog eens overgedaan, maar dan met iedereen erbij. Zo kan er 'live' bepaald worden waar gaten in de defensie zitten. Wat het bij veel overheidsinstellingen lastig maakt, is dat er geen sprake is van één overkoepelende IT-infrastructuur, het zijn allemaal losse eilandjes binnen verschillende afdelingen of diensten. Er wordt bovendien niet altijd optimaal samengewerkt. Aan de andere kant worden er al grote stappen gezet. Waren de meeste overheden tot enkele jaren geleden onbewust van hun daadwerkelijke weerbaarheid tegen cyberaanvallen, intussen is er door het uitvoeren van Red Teamings meer bewustzijn gecreëerd. En dat is een enorme stap: alleen als je weet dat er een lek is, kun je beginnen met het dichten. Daar is nog wel deels een cultuurverandering voor nodig. Vaak legt de IT-afdeling de verantwoordelijkheid voor veiligheid bij de securityafdeling. Zij hebben echter vooral een controlefunctie. Echte veiligheid betekent dat het eigenaarschap daarvoor gedeeld wordt. IT-afdelingen én gebruikers zijn daarbij de eerste verdedigingslijn.

Hoe kunnen we je helpen?

Bij KPMG helpen we organisaties met het in beeld brengen van hun huidige cybersecurityvolwassenheids-niveau en stellen we gedetailleerde roadmaps op om naar het gewenste niveau te komen. Daarnaast voert ons Red Team de meest realistische cyberaanvals-imulaties uit waardoor organisaties diepgaand inzicht krijgen in hun effectieve weerbaarheid, samen met de meest relevante bevindingen en aanbevelingen. Want alleen samen maken we Nederland weerbaarder. We praten graag verder over alle mogelijkheden.

Contact

Meer informatie?

Bent u benieuwd naar meer details of heeft u andere vragen? Wij gaan graag met u in gesprek. Neem contact op met een van onze experts.

Ronald Heil

Partner

heil.ronald@kpmg.nl
T +31 (0)20 656 60 33

Jordi van den Breekel

Senior Manager

vandenbreekel.jordi@kpmg.nl
T +31 (0)20 656 72 64

www.kpmg.nl

November 2023