Toets je cyberweerbaarheid aan de praktijk

6 stappen om securityrisico's en besluiten met je stakeholders te bespreken

Beveiligingssoftware, toegangsbeheer en monitoring helpen je organisatie beschermen tegen cyberaanvallen. Maar de aanwezigheid van die maatregelen vertelt nog niet hoe goed ze samen werken. Als een aanvaller een account van een medewerker overneemt, wil je weten welke systemen en gegevens bereikbaar zijn, of afwijkend gedrag wordt opgemerkt en wie mag ingrijpen.

Met ons stappenplan onderzoek je dat voor één kritisch bedrijfsproces, zoals orderverwerking, productie of patiëntenzorg. Je brengt afhankelijkheden in kaart, werkt een aanvalsscenario uit en toetst hoe detectie en opvolging zijn geregeld. Zo maak je zichtbaar wat aantoonbaar werkt en welke aannames nog onderzoek vragen.

Hoe je het stappenplan gebruikt

- Als IT-afdeling bereid je de technische informatie voor en bespreek je de uitkomsten met de procesverantwoordelijke, management/directie en Finance.
- Samen bepaal je welke gevolgen een security-incident kan hebben en welke verbeteringen voorrang verdienen.
- Werk de uitkomsten per stap uit in een eigen document of gebruik de opdrachten als agenda voor een gezamenlijk overleg met je stakeholders.
- Leg de besluiten, actiepunten en wie ermee aan de slag gaat vast.

#1 Breng afhankelijkheden en bedrijfsimpact samen

Samen met applicatiebeheer, de procesverantwoordelijke en Finance

Een aanval op een applicatie kan gevolgen hebben voor een heel bedrijfsproces. Als de orderverwerking stilvalt, kunnen medewerkers bijvoorbeeld ook geen leveringen voorbereiden of klanten informeren.

Begin daarom bij één proces en breng samen met de procesverantwoordelijke in kaart welke systemen, gegevens en leveranciers daarvoor onmisbaar zijn. Ook de inlogvoorziening en koppelingen met andere applicaties horen daarbij.

IT maakt de afhankelijkheden zichtbaar, de procesverantwoordelijke en Finance helpen vervolgens om de gevolgen van uitval, datadiefstal of ongewenste wijzigingen te bepalen. Zo wordt duidelijk welke dienstverlening moet doorgaan en waar verstoring de organisatie het hardst raakt.

Leg vast: het gekozen proces, de kritieke afhankelijkheden en de verwachte gevolgen van een incident. Benoem waarop je die inschatting baseert en wie de ontbrekende informatie aanvult.

#2 Onderzoek wat een overgenomen account kan bereiken

Samen met je securityspecialist(en), applicatiebeheer en de procesverantwoordelijke

Een account van een medewerker kan toegang geven tot informatie en functies die iemand voor het werk nodig heeft. Maar wat kan een aanvaller ermee zodra die het account overneemt? Dat onderzoek je samen met de securityspecialist(en) in je organisatie, applicatiebeheer en de procesverantwoordelijke.

Volg de toegang vanuit één account door de betrokken applicaties. Er kan naar boven komen dat rechten ruimer zijn dan nodig of dat gekoppelde systemen toegang bieden die niet direct zichtbaar is. Vanuit dat bereik werk je een aanvalsscenario uit. Zo kun je beoordelen welke maatregelen toegang bemoeilijken en welke de schade beperken wanneer een aanvaller toch binnenkomt.

Leg vast: wat de aanvaller met het gekozen account kan bereiken, welke maatregelen dat begrenzen en welke rechten of aannames nog controle vragen.

#3 Bepaal welke aanvalssignalen zichtbaar moeten zijn

Samen met securityspecialist(en) en met je securitydienstverlener

Om dit scenario te herkennen, moet je weten wat "opvallend gedrag" is. Bij misbruik van een account kan dat bijvoorbeeld een ongebruikelijke inlogpoging zijn, gevolgd door het raadplegen van veel meer dossiers dan normaal. De waarde zit dan ook in het verband tussen die gebeurtenissen.

Onderzoek met je securityteam of dienstverlener welke informatie beschikbaar is en wie die kan beoordelen. Daarbij tellen ook de bewaartermijn en toegankelijkheid van logs mee. Gebruik je Extended Detection and Response (XDR) om signalen te combineren? Controleer dan of de benodigde bronnen daadwerkelijk zijn aangesloten en voldoende informatie leveren voor onderzoek.

Maak concreet: welke bevindingen moeten beschikbaar zijn om verantwoord door te kunnen gaan?

#4 Maak bevoegdheden bij ingrijpen expliciet

Samen met securityspecialist(en), management en de procesverantwoordelijke

Krijg je een verdachte melding, dan wil je snel handelen. Toch is een systeem isoleren geen vanzelfsprekend besluit wanneer daardoor ook de orderverwerking stopt. Je moet vooraf weten welke ruimte je IT-afdeling heeft om te handelen en wanneer het management/de directie of de procesverantwoordelijke moet beslissen. Bespreek daarom hoe je vanuit de eerste melding tot een actie komt. Daar horen afspraken bij over onderzoek, toestemming en uitvoering, ook wanneer een externe securitypartij betrokken is. Die afspraken moeten ook werken buiten kantooruren en wanneer de vaste contactpersoon niet bereikbaar is.

Spreek ook af wie beoordeelt of een incident meldplichtig is en wie de melding uitvoert.

- Een meldplichtig datalek moet onder de AVG zonder onnodige vertraging en uiterlijk binnen 72 uur na kennisname bij de Autoriteit Persoonsgegevens worden gemeld.
- Voor organisaties die onder de Cyberbeveiligingswet (NIS2) vallen, geldt bij significante incidenten in beginsel een vroegtijdige waarschuwing binnen 24 uur en een incidentmelding binnen 72 uur na kennisname.

Leg vast: welke acties IT direct mag uitvoeren, waarvoor toestemming nodig is en wie beslist. Dus ook wie vervanging waarneemt en welke afspraken je maakt met externe partijen. Benoem ook wie de meldplicht beoordeelt, wie meldt en wie de termijnen bewaakt.

#5 Toets de hele keten van signaal tot ingrijpen

Samen met securityspecialist(en) en de betrokken uitvoerders

Op papier kunnen de afspraken kloppen, terwijl een melding in de praktijk niemand bereikt. Een gezamenlijke oefening helpt om de opvolging te doorlopen. Met een technische test, bijvoorbeeld een gecontroleerde gesimuleerde aanval, toets je of de verwachte signalen daadwerkelijk ontstaan. Betrek hierbij ook je externe securitydienstverlener, als die een rol heeft in detectie of opvolging.

Stem de uitvoering vooraf af met de betrokken beheerders en uitvoerders. Tijdens de toets volg je wat er werkelijk gebeurt. Ontstaat het verwachte signaal, krijgt de juiste persoon voldoende informatie en kan de afgesproken actie worden uitgevoerd? Zo zie je waar de keten werkt en waar nog iets ontbreekt.

Leg vast: noteer de testdatum, bevindingen en verwijzingen naar bewijs. Maak onderscheid tussen wat is aangetoond en wat nog onderzocht moet worden.

#6 Toets de hele keten van signaal tot ingrijpen

Samen met management, Finance en de procesverantwoordelijke

De uitkomsten geven je IT-afdeling een concrete basis voor het gesprek met management en Finance. Je kunt nu uitleggen welke tekortkoming het bedrijfsproces blootstelt aan risico en wat een verbetering daaraan verandert.

Bespreek welke inzet en kosten nodig zijn, maar ook welk risico blijft bestaan wanneer de organisatie uitstelt. De bevoegde beslisser kan daarmee een afgewogen keuze maken voor uitvoering, een alternatief of het accepteren van het resterende risico. Bij uitvoering hoort vervolgens een nieuwe toets die moet laten zien of de verbetering het effect heeft dat je voor ogen had.

Leg vast: noteer de testdatum, bevindingen en verwijzingen naar bewijs. Maak onderscheid tussen wat is aangetoond en wat nog onderzocht moet worden.

Sparren over je security-aanpak?

Blijkt uit het stappenplan dat je zicht mist op een deel van je omgeving, of twijfel je of detectie en opvolging goed op elkaar aansluiten? Bespreek je bevindingen met Joris Rooijackers, Solution Consultant Security bij Bechtle. Hij kijkt graag met je mee naar welke punten verder onderzoek vragen en welke vervolgstap past bij jouw organisatie.



Joris Rooijackers
Solution Consultant Security
Bechtle BV
joris.rooijackers@bechtle.com

Meer informatie

bechtle