Ransomware Resilience Assessment

De meeste organisaties zijn sterk afhankelijk van informatietechnologie voor hun dagelijkse operaties en om hun missie te vervullen. Een succesvolle ransomware aanval kan deze activiteiten tot stilstand brengen. Gevoelige gegevens kunnen worden gestolen en uitlekken bij dubbele afpersingsaanvallen. **Secura's Ransomware Resilience Assessment toont onze klanten precies hoe kwetsbaar ze zijn voor ransomware-aanvallen en biedt een actiegericht stappenplan voor hoe zij hun weerbaarheid tegen ransomware kunnen verbeteren.**

De opmars en het risico van Ransomware

In de afgelopen jaren is ransomware geëvolueerd van een plaag voor individuen tot een existentiële bedreiging voor de meeste organisaties. De snelle opkomst en groei van ransomware-aanvallen kan worden verklaard door het krachtige en schaalbare verdienmodel dat daaraan ten grondslag ligt. Ransomware-aanvallen resulteren in forse winstmarges voor cybercriminelen zonder een significant risico op aanhouding. Zolang de stimulansen om ransomware-aanvallen uit te voeren groter zijn dan de risico's voor cybercriminelen, zullen **de risico's van ransomware naar verwachting blijven toenemen.**

De ondergrondse wereld achter ransomware-aanvallen bestaat uit diverse actoren die hun diensten aan elkaar as-a-service aanbieden. Een ransomware-aanval begint vaak met ongerichte infecties van individuele systemen met malware op een grote schaal via methodes zoals phishing. De toegang op afstand tot geïnfecteerde systemen biedt cybercriminelen ook een voet tussen de deur tot het IT-netwerk van de getroffen organisaties. Deze toegang tot organisaties kan meerdere malen worden verkocht tussen cybercriminelen voordat er tot een ransomware-aanval wordt overgegaan. De prijs voor de toegang varieert afhankelijk van factoren zoals de sector waarin de getroffen organisaties opereren en hun financiële positie.

De prijs voor de toegang tot organisaties via geïnfecteerde systemen wordt ook bepaald door de mate van (beheer) toegang die is verkregen tot de IT-infrastructuur. Als de mate van toegang initieel beperkt is, dan kan de toegang eerst worden uitgebreid door andere systemen in het netwerk van de getroffen organisatie te hacken. Uiteindelijk wordt de verkregen (beheer)toegang te gelde gemaakt door de IT-infrastructuur en de bijbehorende gegevens van organisaties te stelen en te versleutelen. Daarbij worden organisaties vaak dubbel afgeperst, waarbij betaald moet worden om de gegevens weer toegankelijk te maken, maar ook om te voorkomen dat kritieke gegevens over de organisatie of klanten worden gelekt of verkocht.

Hoe werkt een ransomware aanval?

Ransomware-aanvallen verlopen vaak in drie fases. Eerst proberen cybercriminelen toegang te krijgen tot systemen in netwerken van organisaties. Vervolgens proberen ze meer systemen onder controle te krijgen, door zich binnen die netwerken te verspreiden, om de impact van een ransomware-aanval te vergroten. Tot slot worden gevoelige gegevens gestolen, back-ups vernietigd en systemen versleuteld.

GET IN

Cybercriminelen zullen vaak proberen bekende aanvalsvectoren te gebruiken om willekeurige op het internet aangesloten systemen te compromitteren met malware. De malware biedt ze initieel toegang op afstand tot de netwerken van organisaties. De meest voorkomende aanvalsvector om toegang te krijgen tot netwerken van organisaties is door het gebrek aan beveiligingsbewustzijn van werknemers uit te buiten via phishing-aanvallen. Authenticatiemechanismen zonder twee-factor authenticatie om thuis te werken kunnen, in combinatie met een onveilig wachtwoordgebruik, ook worden gebruikt om binnen te komen. Daarnaast kunnen gebreken in de procedures voor systeem- of patch-management leiden tot de exploitatie van kwetsbaarheden in applicaties die via het internet beschikbaar zijn. **Deze aanvalsvectoren vloeien voort uit de complexe wisselwerking tussen mensen, processen en technologie.** Blootstelling aan één van deze aanvalsvectoren is een eerste stap naar ransomware-aanvallen.

HACK THROUGH

Zodra de initiële toegang tot een netwerk is verkregen, kunnen cybercriminelen die toegang gebruiken **om zich een weg te banen door het netwerk** door interne systemen te hacken op zoek naar hogere privileges. Op deze manier kan de impact van een ransomware-aanval vergroot worden. Onveilige IT-beheerpraktijken, systeem configuratiefouten en een andere kwetsbaarheden kunnen cybercriminelen in staat stellen hun privileges binnen de IT-omgeving te verhogen en zich zo naar andere systemen te verplaatsen. Het strategische doel van cybercriminelen in deze aanvalsfase is het verkrijgen van de hoogste privileges in de IT-omgeving, zoals die van een Windows-domeinbeheerder.

SEEK & DESTROY

Cybercriminelen maken vaak misbruik van de toegang en de rechten die zij hebben verkregen om de back-ups van de getroffen organisaties te beschadigen of te vernietigen. Als de mogelijkheid om de back-ups te herstellen van tafel is, is een organisatie eerder geneigd een hoger bedrag aan losgeld te betalen. Cybercriminelen kunnen ook gevoelige gegevens verzamelen en extraheren om de kans op uitbetaling van losgeld te vergroten en de hoogte van de losgeldeis te verhogen. Zodra hun doelstellingen binnen het netwerk zijn bereikt, wordt de ransomware uitgerold naar alle compatibele systemen waartoe de cybercriminelen toegang hebben verkregen.

Secura's Ransomware Resilience Assessment

Secura heeft een **klantgerichte** en op risico gebaseerde methodologie ontwikkeld om te beoordelen hoe kwetsbaar organisaties zijn voor ransomware-aanvallen en om actiegericht advies te geven om hun cyberweerbaarheid te vergroten. De Ransomware Resilience Assessment bestaat uit meerdere geïntegreerde beveiligingsdiensten die een realistische simulatie vormen van de aanvalspaden die in de praktijk door cybercriminelen worden gebruikt in combinatie met een inventarisatie van de mogelijkheden van een organisatie om daar adequaat op te reageren. Samen maken deze diensten deel uit van een holistische aanpak waarbij de weerbaarheid van de organisatie tegen ransomware wordt bekeken vanuit de perspectieven van mens, proces én techniek.

MENS

Laten we beginnen met de menselijke factor. Werknemers kunnen de zwakste schakel zijn in de beveiliging van een organisatie, maar ze kunnen ook optreden als de eerste verdedigingslinie tegen ransomware-aanvallen. **In de Ransomware Resilience Assessment wordt het bewustzijn van uw medewerkers beoordeeld door middel van een gecontroleerde (gesimuleerde) phishingaanval**.

Op basis van onze uitgebreide ervaring hebben wij verschillende realistische phishing scenario's ontwikkeld. De phishing-simulatie biedt een meetbare en herhaalbare manier om te bepalen hoe het (on)bewustzijn van uw medewerkers bijdraagt aan de algehele weerbaarheid van uw organisatie tegen ransomware. Door middel van de weerbaarheidstest geven wij ook handvatten aan medewerkers hoe zij in de toekomst phishing e-mails kunnen herkennen en melden.

PROCES

Om een organisatie te beveiligen, moet men eerst de bedrijfsprocessen begrijpen. Om de weerbaarheid van uw organisatie tegen ransomware te beoordelen, zullen Secura's experts daarom **vaststellen hoe uw bedrijf kritische processen afhankelijk zijn van specifieke IT en/of OT-systemen en hoe ze verweven zijn met de bredere IT en/of OT-omgeving**. Ook wordt vastgesteld wat de meest waarschijnlijke aanvalspaden voor cybercriminelen zijn. **Daarnaast voeren wij een assessment uit van uw cybersecurity volwassenheid** om een duidelijk inzicht te geven in uw huidige volwassenheidsscore. De beoordeling is gebaseerd op een ransomware-specifiek profiel van het NIST Cybersecurity Framework en omvat elk van de fasen van het omgaan met een aanval: identificeren, beschermen, detecteren, reageren en herstellen. Onze Ransomware Weerbaarheidstest toont u waar zich de gaten zich bevinden en welke stappen genomen moeten worden om het gewenste weerbaarheidsniveau te bereiken.

TECHNIEK

Cybercriminelen kijken vanuit een technisch perspectief naar uw IT-infrastructuur. Dat doen wij ook. **Secura houdt voortdurend de tactieken, technieken en procedures in de gaten die ransomware-groepen gebruiken** om organisaties aan te vallen en wij passen dezelfde modus operandi toe in onze ransomware weerbaarheid penetratietesten.

De reikwijdte van de penetratietesten in de Ransomware Resilience Assessment omvat de volledige IT en OT-infrastructuur die de bedrijfsprocessen van uw organisatie ondersteunt. Wij kunnen uw infrastructuur testen, of deze zich nu op locatie bevindt, in de cloud van uw keuze of een mix van beide.

Onze penetratietesten **richten op de meest waarschijnlijke aanvalspaden** om initieel toegang te verkrijgen tot uw IT-infrastructuur, die verspreiding binnen de IT en OT-infrastructuur mogelijk maken en die gebruikt kunnen worden om gegevens te stelen en te versleutelen.
Door uw IT-infrastructuur te bekijken vanuit de ogen van de cybercriminelen die ransomware inzetten, kunnen wij u voorzien van **waardevol advies om uw infrastructuur en bedrijf kritische processen kosteneffectief te verdedigen** tegen de aanvalspaden die in de praktijk de grootste risico's vormen bij ransomware-aanvallen.

Onze gerelateerde diensten

Secura's Ransomware Resilience Assessment is ontworpen om een grote verscheidenheid aan klanten in verschillende marktsectoren inzicht te geven in hun weerbaarheid tegen ransomware-aanvallen, maar de uitdagingen van elke klant zijn uniek. Gerelateerde diensten die relevant kunnen zijn om de weerbaarheid van uw organisatie tegen ransomware te verhogen, zijn onder meer:

TABLETOP RANSOMWARE CRISISMANAGEMENT

Het beoordelen van uw ransomware weerbaarheid kan helpen om de risico's van een ransomware-aanval te beperken en een calamiteitenplan op te stellen voor het geval het zich toch voor zou doen. Maar weinig calamiteitenplannen overleven een daadwerkelijke ransomware aanval. In Secura's Tabletop Ransomware Crisismanagement, worden de procedures en processen voor het afhandelen van een ransomware incident geoefend en geëvalueerd aan de hand van een realistisch scenario. De geleerde lessen leveren waardevolle feedback om calamiteitenplannen en incident response procedures te verbeteren.

THREAT MODELING WORKSHOP

Applicaties en systemen maken meestal deel uit van een keten van informatie verwerkende systemen. In de interactieve threat modeling workshop met ontwikkelaars, architecten, bedrijfseigenaren en andere belanghebbenden helpt Secura bij het identificeren van mogelijke bedreigingen per component en raakvlak. De mogelijke bedreigingen omvatten maar gaan verder dan ransomware. De workshop verhoogt het beveiligingsbewustzijn en de samenwerking tussen de belanghebbenden en kan hen helpen om zelf ook structureel risico's te identificeren die anders misschien verborgen blijven.

GEDRAGSBEOORDELING

Werknemers bewuster maken van cyberbeveiliging is de eerste stap naar het verbeteren van de weerbaarheid tegen ransomware. De psychologie laat ons echter zien dat er een kloof is tussen bewustzijn en gedrag. Secura's gedragsbeoordeling beoordeelt de drie componenten van het beïnvloeden van gedragsverandering bij uw medewerkers: motivatie, gelegenheid en capaciteit. Met het resultaat van deze beoordeling kunt u uw aanpak optimaliseren om gedragsverandering te stimuleren die de ransomware weerbaarheid van uw organisatie verbetert.

Secura
A BUREAU VERITAS COMPANY

Interesse?

Neem contact op:

Volg ons:

088 888 31 00
info@secura.com
secura.com

BUREAU VERITAS 1828

Shaping a World of Trust