De ultieme checklist voor de preventie en bestrijding van ransomwareaanvallen

2016 is het jaar van de ransomware, aldus een recent rapport van het Institute for Critical Infrastructure Technology (ICIT), een denktank binnen de branche. Bij de bestrijding van ransomware is uw beste aanval een goede verdediging. Is uw organisatie klaar om een aanval af te slaan? Verspil geen uren aan het vinden van een verdedigingsstrategie. Gebruik deze checklist om uw bedrijf te beschermen tegen geraffineerde aanvallen.

☐ 1. Maak back-ups van al uw gegevens

Het krachtigste wapen tegen ransomware is het uitvoeren van regelmatige back-ups. Bij een aanval schakelt u het getroffen endpoint direct uit. Vervolgens plaatst u een nieuwe image op het systeem en herstelt u een recente back-up om te voorkomen dat de ransomware zich verspreidt naar andere systemen in uw netwerk.

Wanneer u ransomware wilt verwijderen, moet u het systeem wissen. Daarom is een back-up van de systeemtoestand of een snapshot essentieel om snel te kunnen herstellen na een aanval. Hoe vaker u een back-up maakt, hoe minder gegevens verloren gaan. De back-upfrequentie moet gebaseerd zijn op het strategisch belang van de gegevens en hoeveelheid gegevens die de organisatie zich kan veroorloven te verliezen. Omdat bij een aanval elk aangesloten apparaat wordt versleuteld, moet de opslag extern zijn en niet zijn toegewezen aan of verbonden met het apparaat nadat de back-up is voltooid.

☐ 2. Patchen, patchen, patchen

Ransomwareaanvallers zijn vaak afhankelijk van mensen die verouderde software gebruiken met bekende kwetsbaarheden die ze kunnen misbruiken om geruisloos in uw netwerk binnen te dringen. Als gevolg van inconsistent patchen en verouderde software zijn organisaties kwetsbaar. Maak er een gewoonte van om uw software regelmatig bij te werken. Door vaak misbruikte software van derden, zoals Java en Flash, te patchen kunt u ongetwijfeld al een groot aantal aanvallen afslaan.

☐ 3. Informeer uw gebruikers over aanvalsbronnen

De zwakste schakel in de beveiligingsketen is meestal de mens. Wanneer een werknemer zich laat misleiden door een phishingbericht of een andere social engineering-tactiek, loopt uw organisatie risico. Informeer uw gebruikers over bedreigingsscenario's op basis van social engineering. Criminelen gebruiken deze tactieken omdat het vaak eenvoudiger is om de natuurlijke neiging van mensen om te vertrouwen te misbruiken dan om manieren te ontdekken om uw software te hacken.

Weten wie en wat u kunt vertrouwen vormt de basis van beveiliging. Train uw gebruikers om zichzelf de volgende vragen te stellen wanneer ze hun e-mail lezen:

1. Ken ik de afzender?
2. Is het echt nodig dat ik dat bestand open of die koppeling volg?
3. Heb ik echt iets besteld bij dit bedrijf?

☐ 4. Bescherm uw netwerk

Beveilig uw netwerk door een gelaagde benadering te implementeren. Gebruik technologieën zoals een firewall van de volgende generatie (NGFW) en een inbraakbeveiligingssysteem (IPS). Een gelaagde verdediging biedt u meerdere mogelijkheden om beveiligingsmaatregelen in meerdere gebieden binnen een netwerk af te dwingen. Wanneer u storingspunten verwijdert, kunt u uw netwerk en gegevens effectief beveiligen en beschermen.

☐ 5. Segmenteer de netwerktoegang

Netwerksegmentering beperkt de hoeveelheid resources waar een aanvaller toegang toe kan krijgen. Het groepeert netwerkactiva, resources en toepassingen op een logische manier in gescheiden gebieden. Wanneer u toegang altijd op een dynamische manier beheert, voorkomt u dat uw hele netwerk via een enkele aanval kan worden besmet.

De meerderheid van de bedrijfsnetwerken is 'plat', met weinig of geen segmentering tussen bedrijfsonderdelen, tussen gebruikers en gegevens, tussen specifieke gegevens van bedrijfsonderdelen, enzovoort. Segmentering kan niet alleen worden gebruikt om de laterale beweging van malware te stoppen of af te remmen, maar ook om bedreigingen in te perken.

☐ 6. Houd netwerkactiviteit goed in de gaten

U kunt geen bescherming bieden voor wat u niet kunt zien. Het verkrijgen van diepgaande zichtbaarheid van het netwerk klinkt mogelijk als een uitdagende taak, maar het is cruciaal. De mogelijkheid om alles te zien wat er in uw netwerk en datacenter gebeurt, kan u helpen aanvallen te ontdekken die de buitengrens omzeilen en uw interne omgeving binnendringen.

Bescherm de buitengrens door een zogenaamde DMZ (demilitarized zone) te implementeren en te versterken. De DMZ is een fysiek of logisch subnetwerk dat de naar buiten gerichte services van uw organisatie bevat en openstelt aan een meestal groter en niet-vertrouwd netwerk zoals het internet. Hiermee voegt u een extra beveiligingslaag toe aan uw LAN (lokale netwerk). Een extern netwerkknooppunt krijgt alleen directe toegang tot servers in de DMZ en niet tot andere delen van uw interne netwerk.

☐ 7. Voorkom initiële infiltratie

Soms openen uw gebruikers in alle onschuld toch besmette sites of e-mailberichten met malvertising, waardoor uw netwerk wordt blootgesteld aan malware. Initiële ransomware-infecties vinden normaalgesproken plaats via een e-mailbijlage of een kwaadaardig downloadbestand. Wanneer u kwaadaardige websites en door aanvallers als onderdeel van hun ransomwarecampagne verzonden e-mailberichten en bijlagen zorgvuldig blokkeert, kunt u uw netwerk blijven beschermen.

U kunt bijvoorbeeld overwegen om te investeren in een door uw bedrijf goedgekeurde toepassing voor bestandsdeling om bestanden uit te wisselen tussen gebruikers in uw organisatie en zakelijke partners. Wanneer u een oplossing met bestandsdeling gebruikt en gebruikers instructies geeft om bestanden nooit via e-mail te delen of te accepteren, kunt u phishing-aanvallen met bijlagen bijna volledig afweren.

☐ 8. Beveilig uw endpoints

Wanneer u een antivirusoplossing op uw endpoints implementeert, biedt dit onvoldoende bescherming tegen ransomware. BYOD (Bring Your Own Device) op de werkplek wordt steeds populairder en dus moet u een oplossing vinden waarmee u controle hebt over de laptops, mobiele apparaten en tablets die verbinding maken met uw netwerk. Het is hierbij essentieel dat uw oplossing twee dingen doet: zichtbaarheid bieden in wat er verbonden is met uw netwerk en u helpen bij het handhaven van beleid dat voorkomt dat gebruikers besmette websites bezoeken of verdachte bestanden downloaden.

Overweeg om het concept van 'minimale bevoegdheden' toe te passen. Hierbij krijgt elke account alleen de minimale bevoegdheden die nodig zijn om relevante taken uit te voeren. Dit concept kan bijvoorbeeld worden toegepast op gebruikersmachtigingen op respectievelijk endpoints en netwerkshares. Momenteel wordt hiervan maar zelden gebruikgemaakt. Het kernpunt van dit concept is dat kwaadaardige software meestal wordt uitgevoerd met het bevoegdheidsniveau van de op dat moment aangemelde gebruiker. Als de gebruiker een beheerder is, dan is de aanvaller dat ook. Gebruik altijd tweeledige verificatie. Een hacker kan wachtwoorden stelen maar het is bijna onmogelijk om tegelijkertijd ook een smartphone of token te stelen.

☐ 9. Verkrijg real-time bedreigingsinformatie

Als u een bedreiging proactief wilt bestrijden, is het belangrijk om uw vijand te kennen. Bedreigingsinformatie biedt beveiligingspersoneel een waarschuwing vooraf over cybercriminelen die zich op hun gebied, branche of zelfs specifieke bedrijf richten zodat u tijd hebt om actie te ondernemen. Dus hoe verkrijgt u real-time bedreigingsinformatie? Door uw oor te luister te leggen en te leren van organisaties die gespecialiseerd zijn in bedreigingsinformatie, zoals Talos.

Het Talos-team bestaat uit meer dan 250 fulltime bedreigingsonderzoekers die zich inspannen om bescherming te bieden tegen bekende en opkomende cyberbeveiligingsbedreigingen. Het team deelt beveiligingsinformatie via blogposts, nieuwsbrieven, sociale media, communityforums en instructievideo's om het internet veiliger te maken voor iedereen. U kunt profiteren van hun werk door hun content op de voet te volgen en binnen uw organisatie maatregelen te nemen wanneer een bedreiging nadert.

☐ 10. Zeg NEE tegen losgeld

Hoewel veel bedrijven in de verleiding komen om losgeld te betalen om de controle terug te krijgen over hun systemen, is dit de allerlaatste optie die u moet overwegen. Neem in plaats daarvan contact op met de autoriteiten en financier deze cybercriminelen niet door losgeld te betalen.

Meer informatie

Ga naar http://www.cisco.com/go/ransomware voor meer informatie over netwerkzichtbaarheid en Cisco Ransomware.