socured
TAKING CARE

©SOCURED

Hybride werken beveiligen

Hybride werken beveiligen

De afgelopen jaren bleven ons tot het uiterste uitdagen. Toen personeel in de meeste sectoren door de pandemie thuis ging werken, zorgde dat voor nieuwe aanvalsoppervlakken waar computercriminelen gebruik van kunnen maken, zoals thuisapparaten die nu voor het werk worden gebruikt. In deze periode vonden drie belangrijke aanvallen plaats: NOBELIUM (de leveringsketenaanval op SolarWinds), HAFNIUM (een aanval op lokale Exchange-servers) en Colonial Pipeline (een ransomwareaanval).

Daar kunnen veel lessen uit worden getrokken. Ten eerste blijven e-mails een dreigingsvector. Phishing is zelfs verantwoordelijk voor bijna 70% van de datalekken. Ten tweede gebruiken criminelen malware die zich voordoet als een legitieme softwareupdate om niets-vermoedende werknemers aan te vallen. Ten derde hebben ransomewareaanvallers de uitdaging nog groter gemaakt door zich naast dubbele of drievoudige afpersing ook bezig te houden met ransomware-als-service (RaaS). Bij RaaS wordt een aanval via een partnernetwerk uitgevoerd, waardoor het lastig is om te bepalen wie de echte aanvaller is. Ten slotte richten kwaadwillenden zich op lokale systemen, waardoor het voor organisaties nog belangrijker wordt om infrastructuur naar de cloud te verplaatsen, omdat de beveiliging daar moelijker te kraken is. Hoewel we van deze incidenten pijnlijke lessen hebben geleerd, is een belangrijke les dat de basis belangrijk is.

> “Phishing is zelfs verantwoordelijk voor bijna 70% van de datalekken.”

Een van de makkelijkste manieren voor criminelen om binnen te komen is een open deur. Als gecompromitteerde organisaties elementaire beveiligingsmaatregelen zoals patches, updates of meervoudige verificatie (MFA) hadden toegepast, waren ze misschien gespaard gebleven of minder zwaar getroffen. Het is eigenlijk schokkend dat minder dan 20% van de bedrijven sterke verificatie zoals MFA gebruikt (terwijl MFA vaak gratis is en standaard kan worden ingeschakeld). Organisaties die deze elementaire beveiligingspraktijken niet toepassen of handhaven, zullen veel meer aan aanvallen worden blootgesteld.

ZERO TRUST-PRINCIPES

Zero Trust elimineert het inherente vertrouwen dat binnen traditionele bedrijfsnetwerken wordt verondersteld. Een effectieve Zero Trust-architectuur is ontworpen om het risico bij elke gelegenheid in het digitale domein te verminderen. In de praktijk betekent dit dat elke transactie tussen systemen voordat zij kan plaatsvinden moet worden gecontroleerd en bewezen betrouwbaar moet zijn.

1. Identiteiten

Identiteiten kunnen mensen, diensten of IoT-apparaten vertegenwoordigen. Als een identiteit een middel probeert te benaderen, moet die identiteit nauwkeurig worden gecontroleerd en moet worden gezorgd dat de toegang aan de regels voldoet en voor die identiteit typisch is. Volg het principe van minimale bevoegdheden.

2. Endpoints

Zodra een identiteit toegang tot een middel heeft gekregen, kunnen data naar verschillende endpoints stromen, van IoT-apparaten tot smartphones, van privéapparaten tot door partners beheerde apparaten en van lokale workloads tot cloudservers. Deze diversiteit creëert een enorm aanvalsoppervlak. Bewaak en handhaaf de apparaatstatus en compliance voor veilige toegang.

3. Applicaties

Applicaties en API's (application programming interfaces) verzorgen de interface waarlangs de data worden gebruikt. Het kan gaan om verouderde lokale applicaties, naar de cloud verplaatste workloads of moderne SaaS-applicaties (softwareals-service). Pas controlemiddelen en technologie toe om schaduw- of niet-goedgekeurde IT te ontdekken, passende machtigingen in apps te waarborgen, op basis van realtime analytics toegang te verlenen, op abnormaal gedrag te monitoren, gebruikersacties te controleren en veilige configuratieopties te valideren.

4. Netwerken

Uiteindelijk worden alle data via netwerkinfrastructuur benaderd. Netwerk-controles kunnen essentiële controlemiddelen bieden om de zichtbaarheid te verbeteren en te voorkomen dat aanvallers zich zijwaarts door het netwerk verplaatsen. Segmenteer netwerken (en pas dieper in het netwerk microsegmentatie toe) en implementeer realtime bescherming tegen bedreigingen, eind-toteindversleuteling, bewaking en analytics.

5. Infrastructuur

Infrastructuur, zowel lokale servers, virtuele machines (VM's) in de cloud, containers als microservices, vormt een kritieke bedreigingsvector. Evalueer softwareversies en configuraties en verleen JIT-toegang om de verdediging te versterken. Gebruik logboekregistratie en bewaking om aanvallen en afwijkingen te detecteren, blokkeer en markeer automatisch riskant gedrag en neem automatisch beschermende maatregelen.

6. Data

Uiteindelijk beschermen beveiligingsteams data. Data moeten tijdens de hele levenscyclus worden beschermd, zelfs als data de apparaten, apps, infrastructuur en netwerken die de organisatie beheert verlaten. Gebruik dataclassificatie en -labels als context voor het versleutelen, minimaliseren van toegang tot, controle over de stroom van en het maskeren of verwijderen van gevoelige informatie aan het einde van de nuttige of wettelijk verplichte levensduur.

"Hackers breken niet in, ze loggen in."

DE NOODZAAK VAN EMPATHIE

Flexibel werken is een blijvertje en dat brengt verschillende uitdagingen en stressfactoren met zich mee. Teams zijn dit jaar meer geïsoleerd geraakt, en digitale uitputting is een echte en onhoudbare bedreiging. Een op de vijf respondenten wereldwijd zegt dat hun werkgever niet om hun werk-privébalans geeft. Vierenvijftig procent voelt zich overbelast. Negenendertig procent voelt zich uitgeput. En uit biljoenen productiviteitssignalen afkomstig uit Microsoft 365 blijkt hoezeer werknemers zich digitaal uitgeput voelen. Een positieve bedrijfscultuur beperkt het risico Uit een recent onderzoek van CyLab, het beveiligings- en privacyinstituut van de Carnegie Mellon University, bleek dat negatieve afschrikking, zoals het beperken, bewaken en straffen van werknemers, niet tegen risico's van binnenuit werkt.

Wat werkt wel?

De betrokkenheid, verbondenheid en het welzijn van werknemers centraal stellen. Om het welzijn van je mensen te ondersteunen, is het belangrijk om kanalen en mechanismen te creëren om naar hun zorgen te luisteren, mogelijkheid te bieden om feedback te geven en ontvangen en samenwerking te omarmen Een holistische benadering op maat waarbij signalen worden samengebracht in een samenhangend beeld van de hele organisatie, geeft meer inzicht in de relevante trends in de organisatie en biedt betere risicobeperking.

Daarom wenden organisaties zich tot ML om verborgen tekenen van werkplekrisico's te ontdekken, zoals ongepaste communicatie, bedreigend gedrag of handelingen die werknemers en het bedrijf kunnen schaden. Door patronen en schendingen te herkennen, kan technologie voor een risico waarschuwen op een moment dat de interventie nog mogelijk is, terwijl we ons blijven inzetten voor de privacy van eindgebruikers.

Ga uit van goede bedoelingen; fouten worden gemaakt.

MEER LEZEN?

Phishing en andere kwaadaardige e-mails

Download

Het dreigingslandschap voor OT en het IoT

Download

BEDANKT VOOR HET LEZEN VAN DEZE WHITEPAPER. HEEFT U NOG VRAGEN OVER HET ONDERWERP?

Neem dan gerust contact met ons op via info@socured.nl of 020 708 55 65.

Socured
Klokkenbergweg 50A
1101 AP AMSTERDAM-ZO
Tel.: 020 708 55 65
info@socured.nl
www.socured.nl

Onderdeel van Socia

Over Socured

Socured is gevestigd in Amsterdam en is onderdeel van Socia. Socia helpt al meer dan 15 jaar haar klanten op het gebied van IT en heeft inmiddels een mooie voetafdruk achtergelaten bij veel bedrijven in Nederland als het gaat om IT-diensten.