Insight Contict

Reference Case | Cloud + Datacenter Transformation

Insight analyseert gecompromitteerde Exchange-server Contict en weet datadiefstal te voorkomen

Contict helpt zijn klanten efficiënt te werken met behulp van ICT. Dit doet Contict door zijn klanten het 'Slimme Werken' aan te bieden. Waar ze zo'n vijftien jaar geleden begonnen met het ondersteunen op telecomvraagstukken, is het aanbod door de jaren heen uitgegroeid naar een totaalpakket aan oplossingen die het bedrijven en mensen makkelijker maakt snel, efficiënt en effectief te werken. Ze maken ICT toegankelijk en werkbaar voor hun klanten en bieden hen een volledige en veilige werkplek in de cloud aan, zonder dat de klant hier omkijken naar heeft.

De uitdaging

Begin maart 2021 waarschuwde Microsoft voor grote beveiligingslekken in Exchange-mailservers en werd er een noodupdate uitgebracht. Tot die tijd konden hackers in mailaccounts komen en eigen software installeren. De gevolgen daarvan konden groot zijn of worden, want het zet de deuren van organisaties wagenwijd open.

"Van een dergelijk bericht schrik je natuurlijk. Wij zijn voor veel van onze klanten het IT-team op afstand en wij ontzorgen hen, daar waar gewenst, volledig op het IT-vlak. Veel van onze klanten maken gebruik van Exchange on-premises servers. Vanaf het moment dat het lek bekend werd, was het direct 'all hands on deck' voor ons. Je wilt zo snel mogelijk weten of de servers besmet zijn of niet. Je wilt de noodupdates checken, doorvoeren en mogelijke bedreigingen isoleren. En dat is wat we ook in rap tempo hebben kunnen doen. Via een tool van Microsoft konden we controleren of er servers geïnfecteerd waren en dat bleek helaas het geval. De impact van de besmetting weet je op zo'n moment echter nog niet, maar we hielden de potentieel getroffen klanten zo goed mogelijk op de hoogte van onze vorderingen," vertelt Ruud Hofmeijer, Netwerkspecialist bij Contict.

Ruud vervolgt: "We konden de besmetting isoleren, maar toch kwam er telkens iets terug. Iets bleef contact zoeken met het internet. We waren er bijna zeker van dat er nog geen data was buitgemaakt, maar bijna is natuurlijk niet genoeg. En wat was er op de server achtergebleven? Kon dat binnenkort alsnog schade toebrengen?

Samenvatting

Na een groot beveiligingslek in de Microsoft Exchange-mailservers ontdekte Contict dat ook hun servers mogelijk waren getroffen. Data leek nog niet te zijn ontvreemd, maar er was wel iets verdachts op de server. Om daar grip op te krijgen schakelden ze Insight in voor onderzoek en advies.

"Vanaf het moment dat het lek bekend werd, was het direct 'all hands on deck' voor ons. Je wilt zo snel mogelijk weten of de servers besmet zijn of niet. Je wilt de noodupdates checken, doorvoeren en mogelijke bedreigingen isoleren."

Ruud Hofmeijer
Netwerkspecialist bij Contict

Contict

"We wilden weten waar die niet-legitieme acties vandaan kwamen, maar we kregen er maar geen grip op. We belden daarom met diverse IT-partners, waaronder ook Insight. Met Insight hebben we normaliter vooral contact rondom licenties, maar onze accountmanager aldaar begreep de ernst van de zaak en schakelde me direct door met beveiligings-specialist Erik Westhovens."

De Oplossing

Na het verhaal te hebben gehoord van Ruud, raadde Erik hem aan zo spoedig mogelijk Azure Defender te installeren. Het beschermt hybride gegevens die worden gehost in Azure, on-premises of in andere cloudservers en detecteert ongebruikelijke pogingen om toegang te krijgen tot opslagaccounts en uploads van malware naar Azure Storage.

"Iedere actie op de server houdt het bij en samen met de logs van de firewall die we al hadden draaien was Erik in staat de besmetting nog beter op te sporen en te isoleren. We waren zo transparant mogelijk en Erik naar ons toe precies zo. In gesprek met hem werd al snel duidelijk dat hij hier echt alles van weet en alles op alles wil zetten om de hack een halt toe te roepen. We hebben ontzettend lang met elkaar aan de telefoon gezeten en samengewerkt. Hij was letterlijk 24/7 beschikbaar en lag er volgens mij net zo wakker van als ik. Door onder andere de logs van Azure Defender naast de logs van onze al bestaande firewall te leggen wisten we alvast zeker dat we inderdaad de besmetting te pakken hadden. Door vervolgens te analyseren wat de besmetting had uitgespookt op het netwerk kon hij uiteindelijk concluderen dat het bij deze besmetting alleen was gebleven. We konden nu ook onze klanten geruststellen. Het bleek namelijk om een 'sleeper cell' te gaan, die door een hacker op elk gewenst moment geactiveerd kan worden voor data-extractie of voor het plaatsen van nieuwe malware. Van beide was nog geen sprake geweest. Zo'n sleeper cell zoekt van tijd tot tijd contact met het internet en dat was wat we dus zagen. Volledig deleten bleek geen optie, maar Erik wist wel de rechten te wijzigen. Admin-rechten waren nu nodig om een datadump te kunnen doen.

Met andere woorden, de sleeper cell was in een permanente slaaptoestand gebracht en niet meer toegankelijk voor hackers. Erik analyseerde ook of er 'lateral movements' waren gemaakt. Zo'n Exchange-server hangt bij klanten in het netwerk en je wilt ook hier met zekerheid weten of het bij deze ene server is gebleven of dat de potentiële malware al dieper het netwerk is binnengedrongen. Dat bleek niet het geval. Zoals ik het nu vertel lijkt het overigens een heel rechtlijnig proces te zijn geweest: scannen, infectie isoleren en klaar, maar dat zijn dit soort dingen natuurlijk nooit. Het is in eerste instantie echt zoeken naar een speld in een hooiberg en een kwestie van trial & error. Allereerst om te vinden waar het signaal daadwerkelijk vandaan komt en vervolgens het doorzoeken van het volledige netwerk op zoek naar laterale bewegingen," zegt Ruud.

"We konden de besmetting isoleren, maar toch kwam er telkens iets terug. Iets bleef contact zoeken met het internet. We waren er bijna zeker van dat er nog geen data was buitgemaakt, maar bijna is natuurlijk niet genoeg. En wat was er op de server achtergebleven? Kon dat binnenkort alsnog schade toebrengen?"

Ruud Hofmeijer
Netwerkspecialist bij Contict

Het Resultaat

Erik Westhovens, Enterprise Security Solution Architect & Evangelist bij Insight voegt toe: "Dit zijn geen alledaagse besmettingen inderdaad en daarvoor zijn geen kant en klare draaiboeken. Nu was Contict niet de enige van onze klanten die getroffen was. De kennis die ik in korte tijd bij iedereen kon opdoen was bijzonder waardevol voor alle partijen. Op het moment dat Ruud mij uitlegde wat er bij hen speelde, wist ik wel dat de klok begon te tikken. Je wilt erger voorkomen. Klanten van Contict wil je kunnen garanderen dat er geen waardevolle data is buitgemaakt, om zo imagoschade van alle betrokken partijen te kunnen voorkomen.

De transparantie die mij werd geboden door Contict heeft er absoluut aan bijgedragen dat we die sleeper cell uiteindelijk volledig aan banden hebben kunnen leggen. “Azure Defender is hierbij een noodzakelijk hulpmiddel, die je talloze data verschaft over wat er op een server allemaal gebeurt. Het lek is via Exchange binnengekomen en ons allemaal overkomen als het ware. Aan dergelijke ondersteuning valt geen prijskaartje te hangen. Wij leren ervan en onze partner helpen we hiermee uit de brand. Dat is voor ons in dit geval meer dan genoeg.”

“Na het vinden en aan banden leggen van de sleeper cell, hebben we toch alle data, minus sleeper cell uiteraard, naar een nieuwe server verhuisd. Je neemt toch het zekere voor het onzekere. Ook hebben we inmiddels alle servers met Azure Defender uitgerust, het heeft zijn waarde meer dan bewezen en het blijkt broodnodig op het moment dat er iets misgaat. Tot op de microseconde hebben we nu inzicht in wat er op alle servers gebeurt, zowel voor, tijdens en na een besmetting. Daar is geen antivirus of firewall tegen opgewassen. Antivirus pakt puur de besmetting, maar Azure Defender doet de rest. Als er nu iets is, zien we het direct. Insight heeft ons hier de basis van meegegeven, de supportdesk kan het nu zelf in de gaten houden. Het geeft ons die extra zekerheid dat de data van onze klanten veilig is. Daar waar wij voor hen dé IT-partij op afstand zijn, is Insight dat zeer zeker ook voor ons,” besluit Ruud.

“Het bleek om een ‘sleeper cell’ te gaan, die door een hacker op elk gewenst moment geactiveerd kan worden voor data-extractie of voor het plaatsen van nieuwe malware. Zo’n sleeper cell zoekt van tijd tot tijd contact met het internet en dat was wat we dus zagen. Volledig deleten bleek geen optie, maar Erik wist wel de rechten te wijzigen.”

Ruud Hofmeijer
Netwerkspecialist bij Contict

Contict Insight

Highlights Resultaten

- Grondige analyse door Insight-team
- Wederzijdse transparantie
- Azure Defender levert data tot op de microseconde
- Data-extractie voorkomen