KUNDENREFERENZ

IS4IT KRITIS

Cyberattacke vom IR-Team rechtzeitig abgewehrt

AUF DIE RETTER IN DER NOT IST VERLASS

> Wir vertrauen beim **Neuaufbau** der **IT-Umgebung** und zukünftigen Sicherheitsarchitektur auf die **Expertise** der IS4IT-Gruppe. Nachdem uns das **IR-Team** dank der enorm schnellen Reaktion und fundierten **Kompetenz** vor massivem Schaden bewahren konnte, sind wir zu **100 Prozent** sicher, den richtigen **Partner** gefunden zu haben.
>
> *Geschäftsführer, Medienunternehmen*

Wenn in den eigenen Systemen plötzlich ein unbekannter Domain Admin im Active Directory (AD) zugange ist, schrillen alle Alarmglocken. So geschah es am 5. April 2023 bei einem mittelständischen Medienunternehmen (Produktion), das daraufhin zunächst selbst fieberhaft mit der Suche nach der möglichen Ursache begann. Der IT-Leiter kontaktierte aber alsbald die IS4IT Kritis und schon beim ersten Krisenmeeting am Gründonnerstag, den 6. April 2023 um 10:00 Uhr wurde klar: Die IT-Infrastruktur ist massiv kompromittiert und Incident Response (IR) unverzichtbar. Nach weniger als einer Stunde war der Auftrag erteilt und das Incident-Response-Team (IR-Team) machte sich auf den Weg Richtung Flughafen. Der geplante Angriff wurde zwar unterbunden, doch die Bereinigung und ein kompletter Neuaufbau der gesamten Infrastruktur führten zu einem umfangreichen Hypercare-Projekt. Dieses nimmt bei über 500 Servern, 700 Workstations und mehreren Standorten entsprechend Zeit in Anspruch. Der Einsatz ist also noch längst nicht abgeschlossen. Trotzdem ist der Kunde sehr froh, dass der Schaden in einem überschaubaren Rahmen blieb.

Phase 1: Ursachenfindung – Forensik im Ersteinsatz

Das IR-Team der IS4IT Kritis stand zunächst vor der typischen Frage jedes betroffenen Unternehmens: „Sind wir infiziert, in welchem Ausmaß und wie lässt sich der Schaden beheben?“ Daher begann um 17:30 Uhr sofort die Suche nach „Patient Zero“, dem Einfallstor in die Systeme des Unternehmens. Die erste Log-Analyse ergab recht schnell, dass die Ursache bei der Virtual Desktop Infrastructure (VDI) lag. Die Schwachstellendatenbank bestätigte das Einfallstor, das vier verschiedene Angreifer mit unterschiedlichem Erfolg nutzten. Die hochkritische Sicherheitslücke in VMware Horizon bestand zudem schon seit Dezember 2022, ohne dass man jedoch die erforderlichen Patches eingespielt hatte. Dieses Versäumnis wurde daraufhin sofort behoben. Darüber hinaus sperrte das IR-Team für das gesamte Netzwerk den Uplink zum Internet, um das Angriffstor zu schließen und weitere Reinfektionen zu verhindern. Das Intranet blieb davon unberührt, sodass die zeitkritischen Produktionsabläufe nahezu störungsfrei weiterlaufen konnten.

Um 21:00 Uhr startete die Suche nach Artefakten für die forensische Analyse. Kopien des Arbeitsspeichers und der Festplatte von „Patient Zero“ wurden dem remote agierenden IS4IT-Forensik-Team zur Verfügung gestellt. Dieses machte sehr schnell die Malware Emotet ausfindig. Hierbei handelt es sich um einen der weitverbreitetsten Trojaner, der im Darknet für Verschlüsselung oder Industriespionage zum Kauf angeboten wird. Weitere Gegenmaßnahmen standen daher auf der Tagesordnung.

ANFORDERUNGEN

- Unterstützung während einer Cyberattacke
- Lokalisierung des Einfalltors, der Malware und betroffenen Systeme
- Umsetzung von kurzfristigen Maßnahmen zur Schadensminimierung
- Bereinigung der Systeme im Hypercare
- Aufbau der neuen, hochsicheren IT-Infrastruktur mit Komponenten zur
  - Verhinderung von Attacken
  - Schwachstellenerkennung
  - Frühzeitigen Erkennung von Angriffen

LÖSUNGEN

- IR-Einsatz in der Krise
- Forensic Services
- Endpoint Detection Response
- Vulnerability Scanning/Vulnerability Management
- Hypercare Services
- Managed SOC Service
- Managed SIEM Service

NUTZEN

- Minimierung des wirtschaftlichen Schadens
- Vor-Ort-Einsatz innerhalb von 6 Stunden nach erstem Kontakt mit IR-Team
- Schnelle Behebung des Sicherheitsproblems zur Verhinderung der Verschlüsselung
- Effiziente Bereinigung der gesamten IT-Infrastruktur
- Aufbau einer Sicherheitsarchitektur für ein konstant hohes Sicherheitsniveau
- Zuverlässige Sicherstellung der frühzeitigen Angriffserkennung in der Zukunft

Phase 2: Schwachstellenidentifizierung – Threat Hunting

Mit IBM Security® QRadar® EDR, dem IBM-Werkzeug für Endpoint Detection and Response, erfolgte das Threat Hunting, d. h. die Analyse sämtlicher Komponenten der Infrastruktur. Es galt, nach und nach hunderte betroffene Server zu bereinigen und gleichzeitig mittels Vulnerability Scanning nach weiteren Schwachstellen bzw. Kompromittierungen zu suchen. Am Karfreitag um 17:00 Uhr – also gut 24 Stunden später – war die VDI-Infrastruktur wiederhergestellt, der Zugriff aufs Internet weitestgehend möglich und der eigentliche IR-Ersteinsatz abgeschlossen.

Jetzt stand das Unternehmen vor der Entscheidung, die Infrastruktur zu behalten oder komplett neu aufzubauen. Im ersten Fall besteht das Restrisiko, dass die Forensiker etwas übersehen haben und es zu einer Reinfektion kommt. Beim Neuaufbau, der parallel zur bestehenden Umgebung durchgeführt wird, fallen unvermeidbare Investitionen an.

Phase 3: Neuaufbau – Hypercare

Da die Kompromittierung des Domain Admins einem gravierenden Domain Takeover gleichkam und insgesamt vier Angreifer lokalisiert wurden, fiel die Entscheidung des Medienunternehmens eindeutig aus: Ein Neustart sollte her, der gleichzeitig auch massive Sicherheitsverschärfungen erlaubt. Derartige Verschärfungen der Security-Vorgaben im Rahmen der Systemnutzung führen zu Mehraufwand für die Anwender und lassen sich aus diesem Grund im Arbeitsalltag oft nur schwer durchsetzen. Aber nach einer konkreten Cyberattacke gab es intern keinen Widerstand.

Getrennt durch zwei Firewalls wurden nach und nach sämtliche Server, Workstations und User komplett sicher und desinfiziert von der alten in die neue Umgebung migriert. Grundlage dafür bildete die sogenannte Bereinigungs-Pipeline, bei der nach einer Inventarisierung von System zu System entschieden wird, ob eine Desinfektion ausreicht oder eine komplette Neuinstallation erforderlich ist. Ältere Systeme beinhalten oft Software, für die es keinerlei Support oder Updates mehr gibt. Da in diesem Fall eine Migration auf eine neue Technologie gar nicht möglich ist, sind zusätzliche forensische Analysen erforderlich. Nur so lässt sich sicherstellen, dass die Systeme frei von Befall sind.

Phase 4: Prävention – Sicherheitsarchitektur erneuern

Auch wenn das Medienunternehmen dieses Mal mit einem blauen Auge davongekommen ist, möchte es natürlich Notfalleinsätze dieser Art zukünftig vermeiden und entsprechende Sicherheitsdefizite weitestgehend beheben. In Zusammenarbeit mit IS4IT Kritis baut das Unternehmen im Rahmen der Migration daher eine komplett neue Sicherheitsinfrastruktur auf, um das Risiko einer weiteren Cyberattacke sukzessive zu minimieren.

Zu den Kernkomponenten dieser Infrastruktur gehören Managed Services der IS4IT-Gruppe wie Managed SOC und Managed SIEM, die frühzeitig mögliche Eindringlinge erkennen und Gegenmaßnahmen einleiten. Ein regelmäßiges Schwachstellen-Scanning stellt sicher, dass Updates zeitnahe eingespielt und Softwarefehler durch Endpoint Detection Response (EDR) unterbunden werden.

Absolute Sicherheit kann jedoch niemand garantieren. Die Erfahrungen von verschiedenen Anwendern belegen aber, dass Fachexpertise in Kombination mit dem Einsatz der passenden Hard- und Software potenzielle Schäden deutlich minimiert.

ÜBER DEN KUNDEN

Branche:	**Medien (Produktion)**
Mitarbeiter:	**über 1000**
Stand:	**November 2023**