Microsoft

Notruf aus dem Krankenhaus

Erpressungstrojaner verschlüsselt sensible Daten – Microsoft Advanced Threat Protection (ATP) spürt ihn auf

Vor jenem Anruf im Oktober 2018 hatte Florian Diebel noch nie etwas von der Windows Defender Advanced Threat Protection (WDATP) gehört. Und auch nicht von der gefährlichen Ransomware GandCrab 5.3, die, wie er am Telefon erfuhr, gerade die IT seiner Klinik angriff. Das musste er auch nicht. Denn der Geschäftsführer der Krankenhaus GmbH Weilheim-Schongau hatte erfahrene Experten zur Seite – sowohl in der hauseigenen IT-Abteilung als auch bei Sepago, einem Microsoft Elite Partner im Bereich Cyber Security. Gemeinsam bekamen sie die Situation innerhalb von nur 72 Stunden in den Griff – drei aufregende Tage mit wenig Schlaf für alle Beteiligten.

Die Herausforderung: Ein unbekannter Angreifer und der Shutdown

„Im Gesundheitswesen und erst recht im Krankenhaus findet vieles digital statt", sagt Florian Diebel. „Aus der Karteikarte von früher ist die digitale Akte geworden. Hat der Patient in der Aufnahme erst mit seiner Gesundheitskarte eingecheckt, läuft über unser Krankenhausinformationssystem KIS alles zusammen. Röntgenbilder, Laborergebnisse, Medikation, OP-Daten. Im Klinikalltag sind wir darauf angewiesen, dass alles reibungslos funktioniert." Mit insgesamt 340 Betten gehören die beiden Kliniken in den oberbayerischen Orten Weilheim und Schongau zu den eher kleinen Häusern. Neben der Notversorgung haben sich die Mediziner über Jahre einen guten Namen in der Endoprothetik, der Gefäßchirurgie und der Akutgeriatrie gemacht. „Unsere geringe Größe ermöglicht uns eine gewisse Exklusivität. Die Menschen in der Region vertrauen uns, wir sind gut ausgelastet." So auch an dem Tag, an dem Florian Diebels Smartphone klingelte. „Die Systeme im Krankenhaus laufen nicht stabil", hieß es. Ein Mitarbeiter hatte leichtfertig den Anhang einer privaten E-Mail geöffnet. Er dachte, es wäre eine Rechnung. Tatsächlich war es aber ein Krypto-Trojaner, der sofort Zugang zu den internen Laufwerken erlangte und damit begann, Files zu verschlüsseln. Rasend schnell mit dem Ziel, maximalen Schaden anzurichten. Immer versehen mit einer Zahlungsaufforderung in Bitcoins. Florian Diebel traf gemeinsam mit seinen IT-Administratoren die Entscheidung, umgehend alle Systeme herunterzufahren. Und das im laufenden Krankenhausbetrieb. „Das lief sehr geordnet. Wir sind vertraut mit kritischen Situationen, schalten uns zusammen, beurteilen die Lage und ergreifen Maßnahmen. Hier kamen wir aber alleine

„Microsoft hatte mit der Windows Defender Advanced Threat Protection das richtige Werkzeug für unser Problem. Und Sepago war der erfahrene Handwerksmeister, der mit diesem Werkzeug umgehen konnte. Dank dieser exklusiven Kombination ist uns die Situation nicht entglitten – wir hatten immer alles unter Kontrolle."

Florian Diebel, Geschäftsführer Krankenhaus GmbH Weilheim-Schongau

KRANKENHAUS GMBH
LANDKREIS WEILHEIM-SCHONGAU

Kunde
Krankenhaus GmbH Landkreis Weilheim-Schongau

Partner
Sepago GmbH

Produkte und Dienste
Microsoft 365 Enterprise

Branche
Health Provider

Unternehmensgröße
Mittel (50-999 Mitarbeiter)

Standort
Weilheim, Schongau

nicht weiter." Die Cyber Security Spezialisten von Sepago wurden alarmiert. Weil die steigende Anzahl vernetzter Geräte immer neue Angriffspunkte auf Unternehmensnetzwerke schafft, bietet die IT-Beratung neben präventivem Security Consulting auch ein sogenanntes Security Operation Center, das im Krisenfall Angreifer aufspürt und eliminiert. Das wichtigste Werkzeug der Cyber Hunter: die Windows Defender Advanced Threat Protection (WDATP) – eine Lösung aus dem Enterprise Mobility + Security Portfolio von Microsoft 365.

Die Lösung: Big Data Echtzeitanalyse, künstliche Intelligenz und eine Verhaftung

„Wir haben unser Incident Response Team zusammengestellt und die Jungs innerhalb von einer Stunde von Köln und München auf die Autobahn Richtung Süden gebracht", sagt Alexander Benoit, Lead Security Analyst bei der Sepago GmbH. Beim Kickoff Meeting im Krankenhaus waren neben Sepago, der Klinikleitung und der IT auch Beamte von Interpol dabei – ein Standardprozedere bei zur Anzeige gebrachten Cyberangriffen. „Im ersten Schritt haben wir die cloudbasierte WDATP ausgebracht, um zu verhindern, dass sich der Schädling weiter ausbreitet", so Benoit weiter. Die Suche nach „Patient 0" begann – so wird der Rechner genannt, der zuerst befallen wurde. Als der gefunden und der Schadcode extrahiert war, übernahm das Security Operation Center von Sepago in Köln mit der IT-Forensik. „Unsere Cyber Security Experten haben die Nacht durchgearbeitet. Sie nutzten die verhaltensbasierte Erkennung von Windows Defender mit Advanced Hunting. Immer wieder standen wir auch im direkten Kontakt mit den Microsoft Entwicklerteams in Israel – ein Service, den nur Microsoft Elite Partner bieten können: Wir haben einen sehr engen Kontakt zu Microsoft und intensiv Feedback bei der Weiterentwicklung der Lösung eingebracht. Über die Machine Learning Module in der Azure Cloud konnten wir den Schädlingstyp GandCrab 5.3 identifizieren und schnell Maßnahmen ergreifen." Schon am Abend des zweiten Tages fing Sepago nach Bereinigung und Recovery an, die Umgebung sukzessive wieder hochzufahren. „Die Patienten haben von alldem nichts bemerkt", sagt Florian Diebel. „Wir haben auf Handbetrieb umgestellt: Die Gesundheitskarten kamen nicht ins Lesegerät, sondern wurden abgeschrieben. Jede Information wurde handschriftlich festgehalten und anschließend im System nachgetragen – das hat uns einiges an Zeit gekostet. Aber ansonsten ist nichts passiert. Wir haben keinerlei Daten verloren." Alexander Benoit lobt das gute Backup-Management des Krankenhauses: „Die Sicherung ist komplett getrennt von der Arbeitsumgebung – das ist eher selten. Außerdem hat die IT extrem schnell und gut reagiert."

Nicht nur während der kritischen 72 Stunden hielt Florian Diebel seine Belegschaft über den aktuellen Stand auf dem Laufenden. Auch im Nachgang machte er den Vorfall transparent – in Betriebsversammlungen, im Mitarbeiter-Magazin, in Führungskräfte-Meetings. „Wir haben die IT-Sicherheit ganz oben angestellt. Der Vorfall hat uns gezeigt, was es bedeutet, angreifbar zu sein", sagt Diebel. Seitdem sind kritische Systeme konsequent mit WDATP ausgestattet – der nächste Schritt ist der Rollout von Office 365 Advanced Threat Protection und Azure Advanced Threat Protection, um die Krankenhäuser in Weilheim und Schongau vor ähnlichen oder gar schlimmeren Angriffen zu schützen. „Moderne Schadsoftware ist polymorph", warnt Stratos Komotoglou, Manager Modern Workplace Security bei Microsoft Deutschland. „Sie kann bei Übertragung auf ein Gerät ihre Form verändern, und ist dadurch nur schwer von herkömmlichen Antivirenprogrammen zu entdecken. Um sich vor hochentwickelten Gefahren zu wappnen, müssen Unternehmen zeitgemäße Anti-Phishing-Lösungen implementieren, die auch auf solche Angriffe vorbereitet sind und hierfür Technologien wie künstliche Intelligenz (KI) und Machine Learning (ML) einsetzen."

„Mit dem vollumfänglichen Ansatz von Microsoft Threat Protection über schützenswerte Identitäten, Endpunkte und Produktivitätslösungen und die verhaltensbasierte Erkennung zum Beispiel von Schadcode bietet Microsoft einen einzigartigen Schutz für Unternehmen. Sepago unterstützt dabei, sowohl die Lösungen als auch das Security Team optimal auf die heutige Bedrohungslage auszurichten."

Alexander Benoit, Lead Security Analyst, Sepago GmbH, Köln

Und noch zwei Personalien zum Happy End: Der Mitarbeiter, der die Malware freigesetzt hat, arbeitet immer noch im Haus und ist nun sehr sensibel was das Öffnen von Dateianhängen angeht. Und: Nur kurze Zeit nach dem Angriff klickten irgendwo in Osteuropa die Handschellen: Interpol konnte den verantwortlichen Hacker ausfindig machen. Dank Sepago und Windows Defender Advanced Threat Protection von Microsoft.

KRANKENHAUS GMBH
LANDKREIS WEILHEIM-SCHONGAU

Kunde
Krankenhaus GmbH Landkreis Weilheim-Schongau

Partner
Sepago GmbH

Produkte und Dienste
Microsoft 365 Enterprise

Branche
Health Provider

Unternehmensgröße
Mittel (50-999 Mitarbeiter)

Standort
Weilheim, Schongau