inside-it.ch

Mittwoch, 03.07.2019

Offix von massivem Hacker-Angriff getroffen

Das Ransomware-Trio Emotet, Trickbot und Ryuk hat die IT-Systeme der Offix-Gruppe lahmgelegt. CEO Martin Kelterborn erklärt den Ablauf des Hackerangriffs im Gespräch mit inside-it.ch.

Die Systeme der Unternehmen von Offix wurden "durch einen gezielten, geplanten, massiven und durchorchestrierten Hacker-Angriff lahmgelegt", informierte die Unternehmensgruppe ihre Kunden im Mai. Die Gruppe, zu der unter anderem Ecomedia und Oridis gehören, wurde praktisch lahmgelegt. Mittlerweile habe man die IT wiederaufbauen können und im Gespräch gibt CEO Martin Kelterborn einen Einblick in den Ablauf des Ransomware-Angriffes. Man wolle offen und transparent über den Angriff kommunizieren, um damit andere Firmen für solche Angriffe zu sensibilisieren. Er erklärt, wie man mit etwas Glück doch noch Zugriff auf ein Backup hatte und mit welchen Notlösungen man die Kunden während des Angriffes bedienen konnte.

Eingedrungen ist die Malware Emotet getarnt als Word-Macro am 15. Mai. Die Schadsoftware kann weitere Schadprogramme nachladen. Im Fall von Offix hat es sich um Trickbot gehandelt. Trickbot ist auf das Ausspähen von Kontozugangsdaten spezialisiert und gibt diese Informationen dann an die Ransomware Ryuk weiter, die als letzte nachgeladen wird. Das Ransomware-Trio Emotet, Trickbot und Ryuk ist kein Unbekanntes und treibt seit Jahren sein Unwesen.

In der Nacht auf Freitag, dem 17. Mai hätten die IT-Security-Systeme zwar Alarm geschlagen, so Kelterborn, aber es sei bereits zu spät gewesen da das Citrix-System für einen Fernzugriff auf die Systeme bereits lahmgelegt gewesen sei. Nachdem im Laufe des Freitags das Ausmass des Angriffs ersichtlich geworden sei und laufend weitere Systeme nicht mehr funktionierten, habe man alle Systeme um 16.00 Uhr heruntergefahren.

Verschonte Linux-Server

Wie Kelterborn weiter ausführt, sei ein Grossteil der IT-Systeme betroffen gewesen, jedoch mit Ausnahmen: alle Linux-Server und das Warenwirtschaftssystem. Da die Webshops auf den Linux-Servern laufen, hätten diese immer funktioniert. Ausgefallen aber seien etwa Zeiterfassung, Saläradministration, Bilddatenbanken, Telefon-Server, Citrix-Server, Exchange Server, eigentlich so ziemlich alles, zählt Kelterborn auf. Auch hätte die Malware viele EDI-Schnittstellen zerstört über die Grosskunden ihre Bestellungen einspielen.

Man sei "faktisch tot" gewesen. Dies obwohl man zu Jahresbeginn die IT-Security noch von externen Experten überprüfen lassen habe, erklärt der CEO. Dabei sei das Fazit gut gewesen, "State of the Art" habe es geheissen.

Da Trickbot darauf spezialisiert ist, Informationen zu sammeln und zurückzusenden, konnte er höchste Admin-Rechte erlangen und mit diesen in den "Systemen herummarschieren", wie der CEO die Aktivitäten der Hacker beschreibt. Da nützen auch mehrfach gespiegelte und an verschiedenen Orten gespeicherte Backups nichts, antwortet er auf die Frage, ob die Backups ebenfalls betroffen gewesen seien.

Krisenmanagement und Notlösungen

Das Krisenmanagement im Unternehmen habe sehr gut funktioniert, lobt Kelterborn sein Team. Im Grunde hätten sämtliche Mitarbeitende zwischenzeitlich für eine von zwei Abteilungen gearbeitet: entweder um die IT zu unterstützen oder um dem Verkauf unter die Arme zu greifen. So habe man mit einer ans Militär erinnernden Organisation die Wertschöpfung einigermassen aufrechterhalten können.

Auf die Schnelle habe man 15 Notebooks gekauft, GMX-E-Mail-Adressen eingerichtet und eine ad hoc Website programmiert. So habe man innerhalb von Stunden einen wichtigen und wertvollen Kanal einrichten können, um die Kunden zu informieren.

Als externer Security-Spezialist wurde die Firma Infoguard an Bord geholt. Die Experten hätten einen sehr guten Job gemacht und helfen können. Nach einer "Weltuntergangsstimmung" am Samstag, habe es am Sonntag gute Nachrichten gegeben.

Einerseits hätten die Hacker einen Fehler gemacht und den Zugang zu einem Backup zerstört, auf das man selbst noch Zugriff gehabt habe. Dieses sei rund eine Woche alt gewesen. Auch ein IT-Partner habe zur Überraschung aller noch über ein altes Schnittstellen-Backup verfügt, wie man erfahren habe. Mit diesen beiden Sachen habe dann etwas Hoffnung bestanden. Man habe die beiden Backups aber verschlossen gehalten, führt Kelterborn aus. Denn die Schadsoftware sei noch sehr lange im Netzwerk gewesen. "So lange man nicht weiss, wo der Virus ist, sind alle Sanierungsmassnahmen obsolet."

Forderung von 45 Bitcoin

Das geforderte Lösegeld zu bezahlen, kam für Kelterborn nicht ernsthaft in Betracht. Dennoch wollte man sich zu Beginn alle Optionen offen halten. Aber es sei bekannt, dass Trickbot nicht nur verschlüsselt, sondern auch Daten löscht. Verlangt hätten die Erpresser 45 Bitcoin, also zum damaligen Kurs rund 330'000 Franken. Lange habe man nicht mit den Erpressern verhandelt. Ironischerweise, so Kelterborn, hätten die Hacker über den E-Mail-Provider Protonmail kommuniziert, also auf Schweizer Technologie für die

Kommunikationsverschlüsselung gesetzt.

Die Melde- und Analysestelle Informationssicherung des Bundes (Melani) habe das Unternehmen rund eine Woche nachdem das bösartige E-Mail eingetroffen war, darüber informiert, dass es noch immer bösartige Aktivitäten aus dem Netzwerk gebe. Gefunden habe man die Malware schliesslich auf einem Touchscreen im Wareneingang. Die Malware habe sich dort versteckt und versucht, Schadsoftware nachzuladen. Jedoch ohne Erfolg.

"Mit an Sicherheit grenzender Wahrscheinlichkeit" seien keine Daten entwendet worden, weil die DNA des Angriffs auf zerstören und verschlüsseln aus war. Mittlerweile seien die IT-Systeme "up and running" und man könne arbeiten, plane aber eine Neuaufgleisung der IT-Security, so Kelterborn. Daneben habe die Gruppe einen Beauftragten IT-Security ernannt. Die Mitarbeiter werden weiter sensibilisiert und man plane Kampagnen. Ausserdem will das Unternehmen die eigenen Systeme mit Intrusionstests regelmässig überprüfen lassen, zählt der CEO einige der Massnahmen auf, die nun ergriffen werden.

Zur Urheberschaft könne er sich nicht äussern. "Dies wäre reine Spekulation", sagt Kelterborn. Und auch den finanziellen Schaden könne er nicht beziffern – "sehr, sehr teuer", sei die Sache aber bestimmt. Ein solcher Angriff gehe natürlich nicht spurlos an einem Unternehmen vorbei. Man warte noch auf Informationen der Versicherung. Eine spezielle Cyber-Versicherung habe die Unternehmensgruppe nicht, aber die "Wiederherstellung von Daten" sei versichert gewesen.

Die Learnings aus dem Angriff seien "zahlreich und werden nun akribisch und konsequent umgesetzt", so Kelterborn als Fazit im Gespräch und listet drei Learnings. Erstens brauche es wieder physisch getrennte Backups, ähnlich, wie man es früher mit Disketten gehandhabt habe. Alles, was am Netz hänge, sei angreifbar. Zweitens müsse man als Unternehmen davon ausgehen, dass man angegriffen wird. Die Frage sei einfach, wie klein der Schaden gehalten werden kann. Drittens müsse man den "Worst Case" planen und nicht auf den "Best Case" hoffen. Kelterborn resümiert: "So viel Glück wie wir hatten, hat man kein zweites Mal." (Katharina Jochum)

Mehr zu diesem Thema:

Ransomware: Erpresser werden gieriger, Angriffe raffinierter
Melani warnt vor Trojaner-Attacke auf Schweizer Firmen-Netzwerke
Emotet: Deutsches BSI warnt vor Welle hochprofessioneller Angriffe