LOCKY WÜTET IN UNTERNEHMEN

Midland IT®

Minden 05/2016 ks

Wir möchten Ihnen heute einen Fall schildern, der leider nicht nur ein theoretisches Beispiel ist, sondern der sich tatsächlich bereits mehrfach in unserem Kundenkreis zugetragen hat. Stellen Sie sich folgende Situation vor: Sie erhalten eine Mail mit einer beigefügten Rechnung. Das ist nicht ungewöhnlich. Sie klicken also selbstverständlich auf den Anhang, doch statt eines Rechnungsanhangs werden in diesem Moment all Ihre Unternehmensdaten über einen mittlerweile extrem intelligenten bösartigen Trojaner verschlüsselt.

Sie haben nicht die geringste Chance diesen Vorgang zu stoppen, Ihre eigenen Unternehmensdaten werden so verschlüsselt, dass nicht einmal Sie selbst noch darauf zugreifen können. Und im nächsten Moment wird Ihnen klar, dass Sie das Opfer krimineller Machenschaften geworden sind: Der vermeintliche Rechnungssteller „bedankt“ sich zu allem Übel für Ihr entgegengebrachtes Vertrauen mit einer Lösegeldforderung.

Und die traurige Wahrheit in diesem Vorfall: Das kann jedem passieren! Die versendeten E-Mails sind kaum als Betrugsversuch zu erkennen.

Wie würden Sie reagieren? Würden Sie den eigenen Fehler offenbaren und der Forderung nachkommen? Wie würden Sie darüber hinaus handeln? Eins wissen wir: Es besteht kein Grund zu falscher Scham. Lassen Sie uns daher etwas Licht in dieses Thema bringen.

Was genau steckt hinter dem Begriff Ransomware?

Ransomware sind Schadprogramme, mit deren Hilfe es dem Angreifer gelingt, jeglichen Zugriff oder die Nutzung Ihrer Unternehmensdaten sowie des gesamten Computersystems mithilfe eines Klicks durch Sie selbst zu verhindern. Gleichzeitig werden sämtliche Daten durch einen fremden Computer verschlüsselt. Für die Freigabe und Entschlüsselung der Daten fordert der Angreifer anschließend von Ihnen ein „Lösegeld“.

Alleine im Juni und Juli letzten Jahres stieg die Zahl der mit dem Schadprogramm angegriffenen Unternehmen um rund 50 Prozent an - verglichen mit den davor liegenden Monaten Mai und April. „Locky“ - der aktuellste Trojaner - toppt alles: Über 5.000 Infizierungen pro Stunde (!) sind bisher gemeldet worden. Der Grund für den sprunghaften Anstieg? Die Entwickler von Ransomware lernen schnell und konzipieren ihre Programme immer raffinierter. Dies betrifft vor allem die Verschlüsselung: Während die hierfür verwendeten Kommunikationsprotokolle in der Vergangenheit relativ konstant waren, werden inzwischen asymmetrische Verschlüsselungsverfahren angewendet, die sich ständig verändern, um eine signaturbasierte Erkennung der Kommunikation zu umgehen. Ein Entschlüsseln ist somit nahezu unmöglich.

Stichwort Reaktion: Was können Sie im Falle einer Attacke tun?

Ziehen Sie auf jeden Fall uns als IT-Expreten zu Rate und bringen Sie den Angriff schnellstmöglich zur Anzeige! Je schneller Sie reagieren, umso größer ist die Chance, die Auswirkungen des Trojaners zu reduzieren. Doch im besten Fall lassen Sie es gar nicht erst dazu kommen.

Stichwort Prävention: Wie können Sie das Risiko eines Angriffs minimieren?

Information
Klären Sie Ihre Mitarbeiter auf und ermutigen Sie sie, im Falle eines irrtümlich geklickten Links schnell zu handeln. Ganz wichtig dabei: Machen Sie Ihren Mitarbeitern klar, dass die Auslösung eines solchen Schädlings jedem passieren kann! Wichtig ist, dass der Ursprung des Trojaners so schnell wie möglich gefunden wird, um längere Stillstandzeiten des Firmennetzwerkes zu verhindern.

Patch Management
Führen Sie automatisierte Updates ein, bzw. kontrollieren Sie die vorhandenen. Nur so garantieren Sie immer den aktuellen Sicherheitsstand der eingesetzten Unternehmensprogramme und Dienste. Wichtig: Dies gilt nicht nur für Microsoft-Produkte, sondern auch für Adobe, Chrome, Firefox, Java & Co..

Regelmäßiges Backup aller Systeme
Der Rettungsanker für den „worst case“: Ein lückenloser Backup Service ermöglicht es Ihnen, Ihre Daten jederzeit wiederherzustellen. Achten Sie dabei auf eine verschlüsselte Auslagerung der Daten an einem zertifizierten Speicherort.

Antivirus und Firewall
Achten Sie auf ein aktuelles Antivirus-Konzept und stellen Sie mit uns Ihre Firewall auf https-Scan um, damit zukünftig auch bei sicherer Kommunikation Tronjaner keine Chance haben.

Mobile Device Mangement
Bedenken Sie dabei: Auch mobile Endgeräte können von Ransomware attakiert werden! Mit Mobile Device Management können Sie dafür sorgen, dass auch Ihre mobilen Geräte besser geschützt sind.

Unser Rat: Besser Sie machen den ersten Schritt!

Die Gefahr, die aktuell von Ransomware ausgeht, ist leider sehr groß. Doch die gute Nachricht: Sie haben es selbst in der Hand, das Angriffspotential im Vorfeld zu verringern. Gern sind wir Ihnen dabei behilflich, geeignete Maßnahmen zu ermitteln und einzuführen.

Midland IT GmbH | Marienstraße 76 | 32427 Minden

Telefon: 05 71 / 9 72 34 – 0 | Telefax: 05 71 / 9 72 34 – 10
E-Mail: info@midland-it.de | Support-Hotline: 05 71 / 9 72 34 – 28

Midland IT®