Asset Management Equity Business
Thematic Insights: Schutz und Sicherheit

Die Renaissance von Ransomware

Dr. Patrick Kolb, Fondsmanager, Credit Suisse

> *„Als ich damals in die Antivirenbranche kam, wurden Updates auf einer 5,25''-Diskette ausgegeben. Seither hat sich vieles geändert."*
>
> *Graham Clulely*

Liebe Leserinnen und Leser,

es war der schlimmste Albtraum eines jeden Systemadministrators. Im April 2016 öffnete ein Mitarbeiter von Lansing Board of Water & Light (BWL) – einem kommunalen Versorgungsunternehmen im US-Bundesstaat Michigan – unbeabsichtigt einen infizierten E-Mail-Anhang und setzte damit einen Computervirus frei. Der Schadcode bahnte sich seinen Weg durch das Netzwerk, verschlüsselte dabei Dateien und machte diese unbrauchbar. Aufgrund des Angriffs war BWL gezwungen, sein Buchführungssystem, sein Mitarbeiter-E-Mail-Programm und sogar seine Telefonleitungen, einschließlich der Kundenhotline, außer Betrieb zu setzen, was zu einer erheblichen Beeinträchtigung seiner Dienstleistungen führte. Zwar wurden keine Einzelheiten zum Virus bekanntgegeben, doch sprach der Generaldirektor von BWL von sogenannter Ransomware – einer Art von Cyberangriff, bei dem Kriminelle den Zugang zu Systemen blockieren, indem sie sie entweder sperren oder Dateien verschlüsseln, bis ein Lösegeld bezahlt wird. „In meinen 40 Jahren in der Geschäftsleitung habe ich so etwas noch nie zuvor erlebt", so der Generaldirektor.[1]

Es ist für das Unternehmen wohl nur ein schwacher Trost, doch BWL ist nicht alleine. Seit Jahresbeginn haben IT-Sicherheitsunternehmen eine Zunahme derartiger Angriffe gemeldet. Experten stellten zudem fest, dass sich der Charakter dieser Angriffe deutlich geändert hat: Konzentrierten sich die Kriminellen in der Vergangenheit noch fast

[1] Network World (2016): „Ransomware attack forces Michigan utility to shut down systems, phone lines, email", 1. Mai 2016, URL: http://www.networkworld.com/article/3063773/security/michigan-utility-shuts-down-systems-phone-lines-email-after-ransomware-attack.html, 19.5.2016.

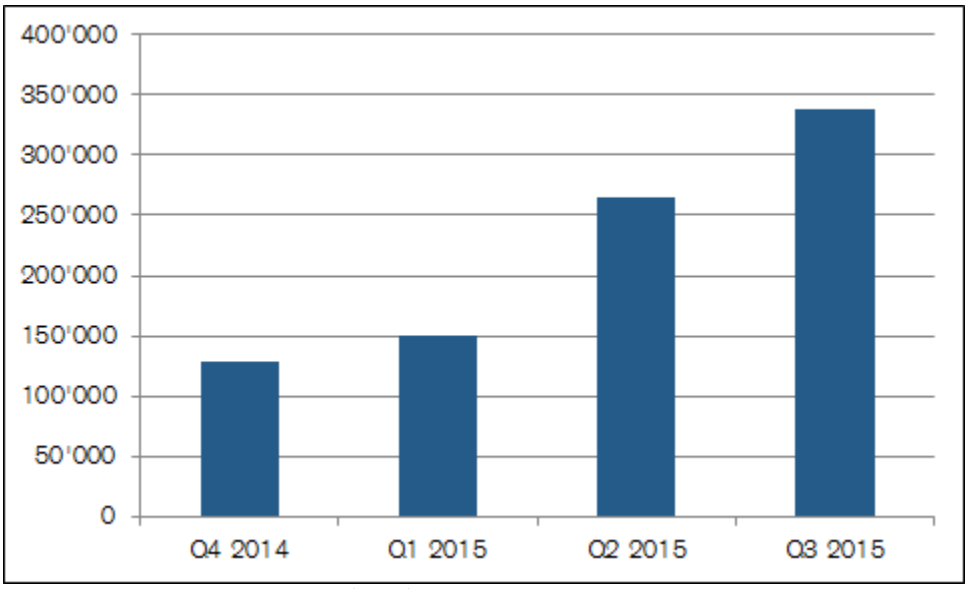
ausschließlich auf Verbraucher, so zielen sie nun immer häufiger auf Unternehmen und wichtige öffentliche und private Organisationen.[2] Dazu zählt eine Reihe öffentlichkeitswirksamer Angriffe auf Krankenhäuser[3] sowie Polizeibehörden. Einige von ihnen waren ironischerweise gezwungen, Kriminelle dafür zu bezahlen, dass sie ihre Strafverfolgung fortsetzen konnte.[4]

Was ist Ransomware?

Ransomware ist nicht neu. Sie trat erstmals im Jahr 1989 in Form des AIDS-Trojaners in Erscheinung, der über Disketten verbreitet und seitdem weiterentwickelt wurde. Die früheren Generationen waren größtenteils gefälschte Antivirenprogramme für Verbraucher oder sperrten die PCs von Privatpersonen, um vermeintlich illegale Dateien zu suchen. Lösegelder von einigen hundert Dollar reichten in der Regel aus, um das Problem zu beseitigen und wieder Zugriff zu erlangen. Aus unterschiedlichen Gründen, einschließlich der Tatsache, dass für die ersten Ransomware-Versionen schnell Gegenmittel gefunden wurden, verkündeten IT-Sicherheitsexperten sogar einen Rückgang dieser Techniken zugunsten anderer Cyberschäden.[5]

Nun nehmen derartige Fälle jedoch wieder deutlich zu, sodass einige gar von einer „Renaissance der Ransomware" sprechen.[6] Die Zahlen bestätigen diesen Eindruck zweifellos. Das Kaspersky Security Bulletin 2015 berichtete, dass sich die Zahl der Kaspersky-Nutzer, die Opfer von Ransomware-Angriffen wurden, zwischen dem 4. Quartal 2014 und dem 3. Quartal 2015 verdoppelt hat (siehe Abb. 1). Im Jahr 2015 wurde Ransomware auf insgesamt 753 684 Computern festgestellt.[7] Proofpoint, ein in den USA ansässiges IT-Sicherheitsunternehmen, hat bei neuen Ransomware-Arten eine Steigerung um mehr als das Vierfache seit Dezember 2015 beobachtet, was zeigt, dass immer mehr Kriminelle in diesen Bereich einsteigen.[8] Laut einer jüngsten Meldung des FBI wurde bei der Strafverfolgung ein Zuwachs von Ransomware im Jahr 2015 festgestellt: „Die ersten drei Monate dieses Jahres lassen darauf schließen, dass die Anzahl an Ransomware-Vorfällen – und die sich aus ihnen ergebenden Schäden – im Jahre 2016 noch weiter zunehmen werden."[9]

Abb. 1: Anzahl der Nutzer, die Opfer eines Ransomware-Angriffs wurden (Q4 2014 – Q3 2015)



Quelle: Kaspersky Security Bulletin (2015), S. 13.

[2] Institute for Critical Infrastructure Technology (2016): „The ICIT Ransomware Report: 2016 Will Be The Year Ransomware Holds America Hostage", 2016, URL: http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report.pdf, 19.5.2016.
[3] Ars Technica (2016): „Two more healthcare networks caught up in outbreak of hospital ransomware", 30. März 2016, URL: http://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware, 19.5.2016.
[4] NBC News (2016): „Ransomware Hackers Blackmail U.S. Police Departments", 26. April 2016, URL: http://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746, 19.5.2016.
[5] ICIT, a. a. O.
[6] Proofpoint (2016): „All Your Data Are Belong To Us", 19. Februar 2016, URL: https://www.proofpoint.com/us/threat-insight/post/All-Your-Data-Are-Belong-To-Us, 19.5.2016.
[7] Kaspersky Security Bulletin (2015): „Overall Statistics for 2015" (Statistik für das Jahr 2015), S. 13, URL: https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/, 19.5.2016.
[8] Proofpoint (2016): „Ransomware Explosion Continues", 27. April 2016: https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered
[9] The Federal Bureau of Investigation (2016): „Incidents of Ransomware are on the Rise", 29. April 2016: https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

Ein Grund dafür, dass Ransomware in kriminellen Kreisen eine derartige Beliebtheit erlangt, ist, dass ein Großteil dieser Schadprogramme nicht sehr anspruchsvoll ist und auf bekannten Schwachstellen oder Sicherheitslücken der Software basiert. Deshalb sind Ransomware-Kits günstig zu erwerben, z. B. im Darknet.[10,11] Doch dies bedeutet nicht, dass Ransomware weniger gefährlich ist. Da diese Malware-Technologie relativ leicht zugänglich ist und ihr Einsatz sich bereits bei einer geringen Erfolgsquote bezahlt macht, werden mehr Übeltäter dazu verleitet, ihr Glück zu versuchen und möglichst viele Ziele anzugreifen.[12] Der mögliche Gewinn ist attraktiv: Mit der Ransomware-Variante Cryptowall wurden Berichten zufolge zwischen 2014 und 2015 mehr als USD 18 Millionen von Opfern erpresst.[13] Und der wachsende Erfolg der Ransomware lockt anspruchsvollere Täter an, was die Entwicklung ernsterer Bedrohungen beschleunigt. Cisco Systems berichtete vor Kurzem beispielsweise von einer neuen Form, bei der Server direkt infiziert werden, anstatt die gewöhnlichen nutzerorientierten Ansätze zu nutzen, wie z. B. Phishing-Kampagnen. Diese spezielle Malware wird offenbar durch die Kompromittierung von Servern verbreitet, die dann als Angriffspunkt genutzt werden, um sich seitwärts durch das Netzwerk zu bewegen und so weitere Geräte zu kompromittieren, die bis zur Zahlung eines Lösegelds gesperrt bleiben.[14]

Die beste Lösung: Seien Sie vorbereitet!

Da ein Großteil der Ransomware momentan noch immer auf bekannte Sicherheitslücken baut, sind größere Unternehmen mit höheren Sicherheitsbudgets diesen Gefahren in der Regel weniger stark ausgesetzt. Für kleinere bis mittlere Unternehmen, kritische Infrastrukturen sowie für wichtige, bekannte Behörden und öffentliche Einrichtungen, die in den zuvor genannten Beispielen erwähnt sind, bestehen erhöhte Risiken. Wir denken, dies liegt daran, dass sie die IT-Sicherheit häufig vernachlässigen und andere Prioritäten setzen, was unter anderem zur Folge hat, dass Sicherheitsupdates und/oder Backups unzureichend sind, man sich auf ältere, anfälligere Systeme verlässt und die Mitarbeiter nicht ausreichend geschult werden.[15] Eine US-Polizeibehörde, die Opfer eines Ransomware-Angriffs wurde, gestand ein, dass sie noch immer mit DOS, einem veralteten Betriebssystem aus den frühen 1980er Jahren, arbeitete.[16]

Unternehmen, die sich gegen die wachsende Ransomware-Flut (und andere Cybergefahren) schützen möchten, müssen zweifellos ihre IT-Sicherheitslandschaft regelmäßig aufrüsten. Die gute Nachricht: Auch wenn sie nicht immer befolgt werden, so sind die allgemeinen Grundsätze einer effektiven Cybersicherheit relativ bekannt. Es gibt eine Reihe von Maßnahmen, die Unternehmen ergreifen sollten.[17] Besonders wichtig ist der Aufbau eines speziellen IT-Sicherheitsteams, das nicht zur normalen IT-Abteilung gehört, mit dieser aber zusammenarbeitet. Dieses Team sollte unter anderem die IT-Risiken beurteilen, einen Cybersicherheitsplan erstellen, gewährleisten, dass dieser korrekt und sorgfältig implementiert wird, und einen soliden Backup-Plan ausarbeiten (Backups gehören zu den besten Schutzmaßnahmen gegen Ransomware, welche Dateien verschlüsselt, da mit ihrer Hilfe das infizierte System schnell wiederhergestellt werden kann, ohne Lösegeld zahlen zu müssen).[18]

Darüber hinaus müssen Unternehmen ihre Schutzmechanismen gegen Cyberattacken fortwährend auf Wirksamkeit und Aktualität überprüfen, insbesondere jene Teile ihrer Systeme, die besonders stark äußeren Gefahren ausgesetzt sind, wie beispielsweise E-Mails oder mobile Geräte. Sie sollten ebenfalls in die Schulung

---

[10] Das Darknet (auch bekannt als Deep Web oder Hidden Web) bezeichnet Teile des World Wide Web, deren Inhalte von Standardsuchmaschinen nicht indiziert werden können. Das Deep Web ist das Gegenteil von Surface Web. Quelle: Greenberg (2014): „Hacker Lexicon: What Is the dark web?“, 19. Nov. 2014, URL: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/, 19.5.2016.

[11] Proofpoint (2016): „All Your Data Are Belong To Us“, a. a. O.

[12] Institute for Critical Infrastructure Technology (2016), a .a. O.

[13] Institute for Critical Infrastructure Technology (2016), a .a. O.

[14] Cisco Systems (2016), „SamSam: The Doctor Will See You, After He Pays The Ransom“, 23. März 2016, URL: http://blog.talosintel.com/2016/03/samsam-ransomware.html, 19.5.2016.

[15] Pacific Crest Securities (2016): „Held for Ransom: Growing Ransomware Threat Could Create SMB Tailwind“, Branchen-Update, 19. April 2016.

[16] NBC (2016): a. a. O.

[17] Siehe Institute for Critical Infrastructure Technology (2016), a. a. O., um einen guten Überblick zu erhalten.

[18] Observer Business and Tech (2016): „How to Beat Ransomware“, 25. April 2016: http://observer.com/2016/04/how-to-beat-ransomware/

ihrer Mitarbeitenden investieren, insbesondere um sie für Social-Engineering-Angriffe, wie z. B. Phishing, die nach wie vor die größte Infektionsgefahr darstellen, zu sensibilisieren. Unternehmen sollten darüber hinaus auch klare Cybersicherheitsrichtlinien und -verfahren entwickeln und überlegen, was im Falle einer Kompromittierung zu tun ist. Da Ransomware häufig eine Lösegeldzahlung innerhalb einer kurzen Frist fordert, raten wir, dass Unternehmen möglichst schnell Reaktionspläne implementieren.

Da diese Maßnahmen wesentlich zum Schutz der Unternehmen beitragen, erfordern sie Know-how und Ressourcen. Dazu gehören spezielle Dienste wie z. B. E-Mail-Scans, Überwachung von Netzwerk und Nutzerverhalten, URL-Blockierung oder Virenprüfung. Natürlich können auch spezielle IT-Sicherheitsunternehmen bei der Sicherheitsplanung und dem Security Workflow unterstützen und bei einem Vorfall helfen, die Daten wiederherzustellen.

Fazit

Unternehmen sollten der IT-Sicherheit stets eine hohe Prioritätsstufe zuweisen. Die traurige Wahrheit ist jedoch, dass viele dies immer noch nicht tun. Im heutigen Umfeld wachsender Bedrohungen und sich häufender spektakulärer Cyberangriffe erwarten wir, dass Regierungen, Unternehmen sowie private Verbraucher langfristig verstärkt in IT-Sicherheitsprodukte investieren werden. Deshalb gehen wir davon aus, dass die Nachfrage nach Dienstleistungen von IT-Sicherheitsunternehmen steigen wird.

Bei der Credit Suisse vertreten wir die Ansicht, dass die Bedrohung durch Ransomware fortbestehen und sich weiterentwickeln wird. Deshalb stellt der allgemeine Markt für IT-Sicherheit ein langfristig ansprechendes Wachstumsthema dar, das mehrere Jahre aktuell bleiben wird, zumal verzweifelt nach Möglichkeiten gesucht wird, sich an den asymmetrischen Vorteil anzupassen, den die Hacker erlangt haben. Darüber hinaus sind wir überzeugt, dass uns die letzte Marktkorrektur im Bereich IT-Sicherheit auf lange Sicht interessante Kaufgelegenheiten bietet.

Letztlich ist das Anlagethema Schutz und Sicherheit unserer Meinung nach sehr reizvoll für langfristig orientierte Anleger und steht erst am Anfang eines attraktiven, langanhaltenden Wachstumszyklus. Aus diesem Grund halten wir Beteiligungen an Unternehmen, die auf dem Gebiet innovativer IT-Sicherheitslösungen wie Security-as-a-Service, Netzwerk- und Endgerätesicherheit, Bedrohungsschutz und Big-Data-Analytik führend sind.

Weitere Informationen (wie aktuelle Fonds-Factsheets, Performanceberichte oder Quartalskommentare) finden Sie hier.

CREDIT SUISSE AG
credit-suisse.com