KURZFASSUNG

Die wirtschaftlichen Folgen von Cyber-Kriminalität – keine Erleichterung in Sicht

Laut einem neuen Bericht von CSIS (Center for Strategic and International Studies) und McAfee verursacht Cyber-Kriminalität weltweit Kosten von fast 600 Milliarden US-Dollar. Das entspricht 0,8 Prozent der weltweiten Wirtschaftsleistung. Der am 21. Februar erschienene Bericht „The Economic Impact of Cybercrime: No Slowing Down“ (Die wirtschaftlichen Folgen von Cyber-Kriminalität – keine Erleichterung in Sicht) bringt die Zahlen des vielbeachteten Berichts von 2014 auf den neuesten Stand. Damals lagen die weltweiten Verluste bei fast 500 Milliarden US-Dollar bzw. 0,7 Prozent der weltweiten Einnahmen.

Die wirkliche Bedeutung dieser Zahl wird klar, wenn man bedenkt, dass sie höher ist als das Bruttoinlandsprodukt der meisten Länder. Und wenn man die Kosten durch Cyber-Kriminalität mit der weltweiten Internet-Wirtschaft (2016: 4,2 Billionen US-Dollar) ins Verhältnis setzt, entspricht Cyber-Kriminalität einer Wachstumssteuer von 14 Prozent.[1]

Im Vergleich der verschiedenen Formen weltweiter Kriminalität belegt Cyber-Kriminalität den dritten Platz hinter staatlicher Korruption und Drogenhandel.[2] Ein schwerwiegendes Problem aus folgenden Gründen:

- **Es betrifft uns alle:** Fast zwei Drittel aller Nutzer von Online-Diensten (insgesamt mehr als zwei Milliarden Menschen) waren bereits von Diebstahl oder Kompromittierung persönlicher Daten betroffen.
- **Geringes Risiko und große Gewinne:** Die Akteure müssen kaum damit rechnen, verhaftet zu werden oder eine Haftstrafe antreten zu müssen. Genau genommen gab es bisher noch kein einziges Urteil zu den schwerwiegendsten Kompromittierungen, die es in die großen Schlagzeilen geschafft haben. Und während die Strafverfolgungsbehörden ihre Bemühungen intensiviert haben, entziehen sich viele Cyber-Kriminellen der Gerichtsbarkeit, indem sie ausschließlich im Ausland agieren.

Wenn man die Kosten durch Cyber-Kriminalität mit der weltweiten Internet-Wirtschaft (2016: 4,2 Billionen US-Dollar) ins Verhältnis setzt, entspricht Cyber-Kriminalität einer Wachstumssteuer von 14 Prozent.[1]

Folgen Sie uns

Laut dem Bericht ist das Cyber-Kriminalitätswachstum von 100 Milliarden US-Dollar darauf zurückzuführen, dass Cyber-Kriminelle neue Technologien schnell einführen.

Außerdem sind die Einstiegshürden in diesem Bereich sehr gering, was durch die wachsende Zahl entsprechender Infrastrukturen begünstigt wird. Zudem gehen die erfolgreichsten Cyber-Kriminellen bei der Abwicklung der finanziellen Aspekte zunehmend raffinierter vor.

Die Fakten

- Ransomware ist das am schnellsten wachsende Tool der Cyber-Kriminellen. Mehr als 6.000 kriminelle Online-Märkte verkaufen Ransomware-Produkte sowie -Dienste, und Ransomware-as-a-Service wird immer beliebter.
- Die Entwicklung von Cybercrime-as-a-Service wird immer weiter vorangetrieben. Auf den florierenden Märkten wird ein breites Spektrum an Tools und Diensten wie Exploit-Kits, angepasste Malware sowie Botnet-Vermietung angeboten.
- Die Maßnahmen von Strafverfolgungsbehörden haben dazu geführt, dass die meisten Geschäfte der Cyber-Kriminellen in das Dark Web verlagert wurden, da die Akteure dort durch Anonymität sowie Kryptowährungen (z. B. Tor und Bitcoin) vor schneller Identifizierung geschützt sind.
- Zu den beliebtesten Malware-Formen im Dark Web gehören Web-Injektionen, Exploit-Kits sowie Infrastructure-as-a-Service, z. B. abgesicherte Hosting-Dienste und Botnet-Vermietungen.
- Mindestens ein Viertel der Kosten durch Cyber-Kriminalität entfällt auf den Diebstahl von geistigem Eigentum. Wenn militärisch genutzte Technologien betroffen sind, ist außerdem die nationale Sicherheit gefährdet.

Bereiche der Cyber-Kriminalität

Der Bericht versucht nicht, die Kosten aller böswilligen Aktivitäten im Internet zu erfassen, sondern konzentriert sich stattdessen auf Kriminelle, die unbefugten Zugriff auf Computer und Netzwerke erlangen. Folgende Bereiche der Cyber-Kriminalität wurden von den Autoren untersucht:

- Der Verlust von geistigem Eigentum und vertraulichen Geschäftsinformationen
- Online- und Finanzbetrug (häufig als Folge gestohlener personenbezogener Informationen)
- Auf börsennotierte Unternehmen ausgerichtete finanzielle Manipulationen
- Opportunitätskosten, einschließlich Produktions- und Service-Unterbrechungen sowie verlorenes Vertrauen in Online-Aktivitäten
- Kosten für den Kauf von Netzwerkschutz, für den Abschluss von Cyber-Versicherungen sowie für die Beseitigung von Schäden nach Cyber-Angriffen
- Rufschädigung und Haftungsrisiken der betroffenen Unternehmen und Marken

Die am schnellsten wachsende Bedrohung

Ransomware greift alle an – große Unternehmen ebenso wie einzelne Verbraucher. Auch wenn nicht alle Opfer das Lösegeld zahlen, lohnt sich das Geschäft dennoch.

Im Vergleich der verschiedenen Formen weltweiter Kriminalität belegt Cyber-Kriminalität den dritten Platz hinter staatlicher Korruption und Drogenhandel.[2]

Laut dem FBI wurden im ersten Quartal 2016 insgesamt 209 Millionen US-Dollar an Lösegeld gezahlt. Im gesamten Jahr zuvor waren es lediglich 24 Millionen.[3] Der explosionsartige Anstieg von Ransomware lässt sich wie folgt begründen:[4]

- Ransomware-Kits werden im Dark Web angeboten. Mehr als 6.000 kriminelle Online-Märkte bieten insgesamt 45.000 unterschiedliche Produkte und Dienste an.
- RaaS-Plattformen (Ransomware-as-a-Service) geben Ransomware-Autoren die Möglichkeit, ihre Reichweite zu vergrößern, indem sie ihren Code gegen Gebühr anderen Cyber-Kriminellen zur Verfügung stellen und eine Provision für gezahlte Lösegelder einstreichen.
- Ransomware-Würmer (z. B. WannaCry) breiten sich in Netzwerken aus und sperren mehrere Computer auf einmal.

Wir erwarten, dass neue Ransomware-Trends auftreten, zum Beispiel Funktionen zur Exfiltration von Daten oder Angriffe auf Mobilgeräte und IoT-Geräte (Internet der Dinge), die meist wenig geschützt sind.

Cyber-Kriminalität weltweit

Der Bericht untersucht Cyber-Kriminalität in Nordamerika, Europa, Zentral-, Süd- und Ostasien, Pazifikraum, Lateinamerika, Karibik, Subsahara-Afrika sowie Nahost und Nordafrika. Die Ergebnisse der Untersuchung zeigen, dass die Kosten durch Cyber-Kriminalität von Region zu Region unterschiedlich sind – je nachdem, wie ausgereift die Cyber-Sicherheitsmaßnahmen im jeweiligen Land sind. Dies wird mithilfe der folgenden Indikatoren ermittelt: rechtliche Maßnahmen, technische Maßnahmen, organisatorische Maßnahmen, Aufbau von Kapazitäten sowie Kooperation.

Die Ergebnisse wurden wie folgt kategorisiert: hochentwickelte Länder mit digitaler Wirtschaft und ausgereifter Cyber-Sicherheit, Länder im Mittelfeld mit sich entwickelnder digitaler Wirtschaft und Cyber-Sicherheit sowie die Länder, in denen die digitale Wirtschaft und Cyber-Sicherheit noch in den Kinderschuhen stecken. Wenig überraschend verzeichnen die wohlhabenderen Staaten höhere Kosten durch Cyber-Kriminalität. Die Folgen von Cyber-Kriminalität sind jedoch in Ländern im Mittelfeld am stärksten spürbar.

- **Brasilien:** Dieses Land ist am zweithäufigsten Ausgangspunkt von Cyber-Angriffen und am dritthäufigsten davon betroffen.
- **Deutschland:** Hier ist die am weitesten entwickelte Internet-Untergrund-Ökonomie der EU beheimatet.
- **Großbritannien:** Online-Betrug und Cyber-Kriminalität machen fast die Hälfte der jährlich mehr als 5,5 Millionen Verbrechen aus.
- **Japan:** Während das Land früher durch die Sprachbarriere und fehlende Geldwäsche-Möglichkeiten geschützt war, nehmen Angriffe (insbesondere auf Banken) in jüngster Zeit zu.
- **Vereinigte Arabische Emirate:** Dieses Land wird weltweit am zweithäufigsten angegriffen. Die Kosten durch Cyber-Kriminalität werden auf jährlich 1,4 Milliarden US-Dollar geschätzt.

Laut dem Bericht ist das Cyber-Kriminalitäts-wachstum von 100 Milliarden US-Dollar darauf zurückzuführen, dass Cyber-Kriminelle neue Technologien schnell einführen. Außerdem sind die Einstiegshürden in diesem Bereich sehr gering, was durch die wachsende Zahl entsprechender Infrastrukturen begünstigt wird. Zudem gehen die erfolgreichsten Cyber-Kriminellen bei der Abwicklung der finanziellen Aspekte zunehmend raffinierter vor.

Schlussfolgerung und Empfehlungen

Auch wenn sich die Analyse von CSIS und McAfee auf die Kosten durch Cyber-Kriminalität konzentriert, nennt der Bericht verschiedene Schritte, mit denen Unternehmen und Staaten die Kosten reduzieren können:

- Einheitliche Implementierung wichtiger Sicherheitsmaßnahmen, z. B. regelmäßige Installation von Updates und Patches für Sicherheits-Software, offene Sicherheitsarchitekturen sowie Investitionen in hochentwickelte Schutztechnologien, die alle Bereiche vom Endgerät bis zur Cloud abdecken
- Stärkere Kooperation bei internationalen Strafverfolgungsmaßnahmen zwischen einzelnen Ländern und privaten Unternehmen sowie Investitionen in zusätzliche Ressourcen zur Untersuchung (insbesondere in wenig entwickelten Ländern)
- Modernisierung aktueller Prozesse wie Rechtshilfeabkommen, mit denen Regierungsbehörden für Untersuchung und Beweissicherung die Unterstützung anderer Länder anfordern können
- Bessere Erfassung aggregierter Daten durch nationale Behörden
- Standardisierung von Bedrohungsinformationen und Koordination von Cyber-Sicherheitsanforderungen zur Verbesserung der Sicherheit in kritischen Bereichen wie dem Finanzsektor
- Schnellere Umsetzung von Abkommen wie dem Budapester Übereinkommen, das die Verantwortung von Staaten bei der Cyber-Kriminalität und die Zusammenarbeit im Bereich Strafverfolgung regelt
- Verhängung vorübergehender Strafmaßnahmen oder anderer Konsequenzen gegen Regierungen, die nicht gegen Cyber-Kriminalität vorgehen

Informationen zu McAfee

McAfee ist eines der weltweit führenden Cyber-Sicherheitsunternehmen, mit Lösungen vom Endgerät bis hin zur Cloud. Inspiriert durch die Stärke enger Zusammenarbeit entwickelt McAfee Lösungen, um eine sicherere Welt für Geschäfts- sowie Privatkunden zu schaffen.
www.mcafee.com/de

1. https://www.bcg.com/documents/file100409.pdf
2. www.imf.org/external/pubs/ft/sdn/2016/sdn1605.pdf
3. Max Metzger: „FBI says Ransomware soon becoming a billion dollar business“ (Laut FBI wird Ransomware bald Milliardenumsätze generieren), SC Media UK, 10. Januar 2017, https://www.scmagazineuk.com/fbi-says-ransomware-soon-becoming-a-billion-dollar-business/article/630615/
4. „McAfee Labs Threats-Report“, McAfee, Dezember 2017.

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de