Acronis

Report 2020

Acronis Cyberthreats Report 2020

Cyber Security-Trends für 2021, das Jahr der Erpressung

Acronis Cyberthreats Report 2020

Inhaltsverzeichnis

AUTOREN:

Alexander Ivanyuk

Senior Director, Product and Technology Positioning, Acronis

Candid Wuest

Vice President of Cyber Protection Research, Acronis

Einführung und Zusammenfassung

Acronis war der erste Anbieter von vollständig integrierter Cyber Protection zum Schutz aller Daten, Applikationen und Systeme. Cyber Protection umfasst die Untersuchung und Überwachung von Bedrohungen sowie die Abdeckung der fünf Vektoren der Cyber Protection: Verlässlichkeit, Verfügbarkeit, Vertraulichkeit, Authentizität und Sicherheit. Im Rahmen dieser Strategie haben wir weltweit drei Cyber Protection Operation Center (CPOCs) aufgebaut, in denen wir rund um die Uhr Cyberbedrohungen überwachen und untersuchen.

Außerdem haben wir unsere aktuellen Flaggschiff-Produkte Acronis Cyber Protect Cloud (Teil der Acronis Cyber Cloud Plattform für Service Provider) sowie die On-Premise-Lösung Acronis Cyber Protect 15 aktualisiert. Bis zu diesem Zeitpunkt war Acronis mit der innovativen Acronis Active Protection Technologie zum Schutz vor Ransomware bereits ein führender Anbieter auf dem Cyber Protection-Markt. Diese Technologie wurde im Laufe der Zeit weiterentwickelt und demonstriert damit die einzigartige Expertise von Acronis bei der Abwehr von Datenbedrohungen. Acronis hat die KI- und verhaltensbasierten Technologien aus dem Jahr 2016 kontinuierlich ausgebaut, um alle Formen von Malware und anderen potenziellen Bedrohungen abzuwehren.

Dieser Bericht deckt die gesamte Bedrohungssituation des Jahres 2020 ab, soweit sie von unseren Sensoren und Analysten erkannt und untersucht wurde.

Die in diesem Bericht vorgestellten allgemeinen Malware-Daten wurden nach dem Start von Acronis Cyber Protect im Mai 2020 im Zeitraum von Juni bis Oktober 2020 erhoben und zeigen die Bedrohungen für Endpunkte, die wir in diesen Monaten entdeckt haben.

Dieser Bericht bietet einen weltweiten Überblick und basiert auf mehr als 100.000 weltweit verteilten individuellen Endpunkten. Erfasst sind nur Bedrohungen für das Windows-Betriebssystem, da sie häufiger auftreten als für macOS. Wir werden weiterhin die Entwicklung der Situation beobachten und im Bericht des nächsten Jahres möglicherweise Daten zu macOS-Bedrohungen aufnehmen.

DIE FÜNF WICHTIGSTEN ZAHLEN DES JAHRES 2020:

- **31 %** der weltweiten Unternehmen werden mindestens einmal am Tag von Cyberkriminellen angegriffen.
- Die Ransomware Maze machte fast **50 %** aller bekannten Ransomware-Fälle aus.
- Bei mehr als **1.000** Unternehmen wurden nach Ransomware-Angriffen Daten geleakt.
- In nur neun Monaten patchte Microsoft fast **1.000** Fehler in den eigenen Produkten.
- Die durchschnittliche Lebensdauer einer Malware-Variante liegt bei **3,4** Tagen.

WICHTIGE CYBER SECURITY-TRENDS FÜR 2021:

- Angriffe auf Mitarbeiter im Home Office werden sich weiter verstärken.
- Datenexfiltration erhält größere Bedeutung als Datenverschlüsselung.
- Die Angriffe auf MSPs, kleine Unternehmen und die Cloud nehmen zu.
- Ransomware wird sich gegen neue Ziele richten.
- Angreifer werden stärker auf Automatisierung setzen und die Zahl der Malware-Varianten wird explodieren.

INHALT DIESES BERICHTS:

- Wichtigste beobachtete Trends bei Sicherheit/ Bedrohungen für 2020
- Allgemeine Malware-Statistiken und Vorstellung der wichtigsten Familien
- Ransomware-Statistiken mit tiefgehenden Analysen der gefährlichsten Bedrohungen
- Kompromittierung vertraulicher Daten als zweite Stufe der erfolgreichsten Ransomware-Angriffe
- Welche Schwachstellen dem Erfolg von Angriffen Vorschub leisten
- Warum MSPs immer stärker bedroht werden
- Sicherheitsprognosen und Empfehlungen für 2021

Teil 1

Schwerwiegende Cyberbedrohungen und wichtige Trends von 2020

1. Angriffe mit COVID-19-Bezug
2. Mitarbeiter im Home Office im Visier
3. Cyberkriminelle konzentrieren sich auf MSPs
4. Ransomware ist immer noch die Bedrohung Nr. 1
5. Einfache Backup- und Sicherheitsfunktionen genügen nicht mehr

Die COVID-19-Pandemie, die Ende 2019 begann, hatte dramatische Auswirkungen auf die ganze Welt. Doch abgesehen von den offensichtlichen Gesundheitsgefahren sowie den wirtschaftlichen Auswirkungen veränderte die Pandemie auch die digitale Welt, unsere Arbeitsweise sowie das Online-Freizeitverhalten.

Als der Reiseverkehr zum Erliegen kam, mussten die meisten Unternehmen und Services auf Online-Betrieb umstellen. Wer bereits online war, musste sein Geschäft ausbauen, während andere vollständig neue Prozesse implementieren mussten. Behörden, Gesundheitswesen sowie Service-Unternehmen mussten neue Methoden einführen, um die alltäglichen Aufgaben erfüllen bzw. unterstützen zu können.

Geschäftliche Meetings wurden nun standardmäßig per Videokonferenzsysteme wie Zoom, Webex und Microsoft Teams abgehalten, während Büroarbeiter häufig eilends und ohne ausreichende Unterstützung nach Hause geschickt wurden, wo sie mit eigenen Geräten arbeiten mussten.

Leider betrachteten die Cyberkriminellen diese Herausforderungen als Chance und steigerten ohne Rücksicht auf Mitgefühl und Moral ihre Angriffsaktivitäten.

1. Angriffe mit COVID-19-Bezug

Wie zu erwarten war, informierten sich die Menschen massenweise im Internet über die neue Pandemie, um sich zu schützen, die neuesten Nachrichten zu erfahren, Hilfsangebote herauszufinden und vieles mehr. Dies führte zu einer Flut von Betrugsversuchen und verschiedenen weiteren Exploits.

Die Cyberkriminellen nutzen weiter die alten schmutzigen Tricks, um das COVID-19-Thema bei ihren Cyber-Angriffen auszunutzen, die Opfer zur Eingabe ihrer Anmeldedaten oder persönlicher Informationen auf Phishing-Webseiten zu verleiten oder Schaddaten in Dokumente zu laden, die wichtige Informationen zur Pandemie enthalten. Es gibt jedoch noch weitere erwähnenswerte Ansätze. Die folgenden Beispiele für Betrugsversuche mit COVID-19-Bezug haben wir tatsächlich beobachtet.

Gefälschte kostenlose Tests

Die neueste Version der Malware Trickbot/Qakbot/Qbot wurde in zahlreichen Phishing-E-Mails verbreitet, die kostenlose COVID-19-Tests anbot. Die Opfer wurden aufgefordert, ein angehängtes Formular auszufüllen, das sich als gefälschtes Dokument mit einem eingebetteten schädlichen Skript erwies. Um die Schaddaten vor Malware-Sandboxes zu verbergen, wird das Skript erst einige Zeit nach dem Download ausgeführt.

Das Köderdokument nutzt eine Standardmethode, um Benutzer zum Aktivieren von Inhalten zu verleiten und damit die Ausführung des eingebetteten schädlichen VBA-Skripts zu starten.

Gefälschte finanzielle Unterstützung

Je nachdem, wie schwer das jeweilige Land von COVID-19 betroffen war, blieben die Cyberangriffe in vielen Fällen lokal. Beispielsweise wurde Nordrhein-Westfalen Opfer einer Phishing-Kampagne. Die Angreifer erstellten gefälschte Kopien der Website des Wirtschaftsministeriums von NRW, auf der COVID-19-Finanzhilfen beantragt werden konnten. Darüber sammelten die Betrüger personenbezogene Daten ihrer Opfer und nutzten sie anschließend in ihren eigenen Anträgen, die sie an die legitime Website übermittelten – ergänzt mit ihren eigenen Bankdaten. Laut Vertretern von NRW wurden bis zu 4.000 gefälschte Anträge gewährt, was zu Schäden von bis zu 100 Millionen Euro führte, die an die Betrüger ausgezahlt wurden.

Betrugsversuche mit Home Schooling

Die Kriminellen nutzten auch Betrugsversuche rund um Home Schooling. Eine neue Phishing-E-Mail mit Pandemie-Bezug verteilte den Trojaner FormBook, der in einer gefälschten Benotungs-App für Schullehrer eingebettet war. FormBook ist eine Infostealer-Malware, die Anmeldedaten aus Internet-Browsern stehlen kann und seit Februar 2016 in Hacker-Foren beworben wird.

Dabei ist interessant, dass die Angreifer mehrere Techniken nutzten, die Analysen und Aufdeckungen verhindern sollen, beispielsweise die Erkennung von Sandboxes und virtuellen Maschinen, Steganografie und XOR-Verschlüsselung. Auf diese Weise konnten sie die Schaddaten verbergen und Windows Defender effektiv unterlaufen.

Von den Kriminellen hinter den FormBook-Kampagnen ist auch bekannt, dass sie Biotech-Firmen angriffen, um Finanzmittel, vertrauliche personenbezogene Daten und geistiges Eigentum zu stehlen.

Gefälschte Freistellung aus gesundheitlichen Gründen

Die Trickbot-Kampagne nutzte ebenfalls die Angst vor der COVID-19-Pandemie aus, um ein Dokument mit dem Titel „Family and Medical Leave of Act 22.04.doc“ zu verteilen (SHA256: 875d0b66ab7252cf8fe6ab23e31926b43c1af6dfad6d196f311e64ed65e7c0ce).

Das US-Gesetz „Family Medical Leave Act“ (FMLA) gibt Angestellten tatsächlich die Möglichkeit, sich aus gesundheitlichen Gründen freistellen zu lassen. Doch sobald der Benutzer das Makro in diesen betrügerischen Dokumenten aktiviert, startet ein böswilliges Skript den Download zusätzlicher Malware auf den Computer.

Eine neue Variante von Sextortion

Wir fanden eine neue Variation des Sextortion-Betrugs. Die Cyberkriminellen nutzen immer noch ein zuvor geleaktes Kennwort als überzeugendes Element, doch anstatt mit der Veröffentlichung eines aufgezeichneten Videos zu drohen, richtet sich die Drohung gegen das Leben des Benutzers. Die Cyberkriminellen behaupten, den genauen Standort und die täglichen Routinen des Opfers zu kennen. Außerdem erklären sie, dass sie „sogar Ihre gesamte Familie mit dem Coronavirus infizieren können“. Um das zu verhindern, fordern sie vom Opfer die Überweisung von 4.000 US-Dollar in Bitcoin.

Dies ist nicht das erste Mal, dass Betrüger das Leben von Benutzern bedrohen. In der Vergangenheit fanden wir Beispiele dafür, dass sie den Opfern mit Schlägern drohten, die sie verprügeln würden. Die COVID-19-Bedrohung hebt das auf ein neues Niveau.

Die meisten dieser E-Mails werden von zufällig gefälschten E-Mail-Adressen oder realen E-Mail-Konten versendet. Natürlich sollte die Nachricht selbst ein deutlicher Hinweis auf einen Betrugsversuch sein, den Sie einfach löschen sollten.

Die Suche nach COVID-19-Geheimnissen von Behörden und Privatunternehmen

Bestimmte wertvolle Daten zur COVID-19-Pandemie, von denen einige Analysten glauben, sie würden von der chinesischen Regierung geheim gehalten werden, haben Hacker aus aller Welt auf den Plan gerufen. Beispielsweise hat die staatlich unterstützte vietnamesische Hacker-Gruppe APT32 (auch als OceanLotus Group bekannt) Medienberichten zufolge staatliche chinesische Organisationen angegriffen, um Maßnahmen zur Virusbekämpfung, medizinische Forschungsergebnisse und geheime Infektionsstatistiken zu erbeuten. Dieses Interesse begründet sich sicherlich zum Teil darin, dass das Nachbarland von China die Ausbreitung der Pandemie unter Kontrolle bekommen wollte.

Das chinesische Unternehmen Huiying Medical wurde gehackt, weil es angeblich anhand von CT-Scans KI-basierte COVID-19-Diagnosen mit 96 % Genauigkeit durchführen kann. Nach Angaben der Cyber Security-Firma Cyble stellte der Hacker „THE0TIME" Daten von Huiying Medical im Dark Web zum Verkauf. Das Paket enthält Benutzerinformationen, Quellcode sowie Dokumentation zu Experimenten. Der Hacker verlangte dafür 4 Bitcoins (zum damaligen Zeitpunkt ca. 30.000 US-Dollar).

Andere ATP-Gruppen griffen Pharma-Unternehmen und Impflabore an, um an relevante Daten zu gelangen.

2. Mitarbeiter im Home Office im Visier

Die COVID-19-Pandemie hat die Bedrohungssituation erheblich verändert und zahlreiche Sicherheits- und Datenschutzrisiken in Bezug auf die Arbeit im Home Office ans Tageslicht gebracht. Dazu gehören der Remote-Zugriff auf interne Unternehmensserver, virtuelle Konferenzen und Sicherheitsschulungen für Mitarbeiter.

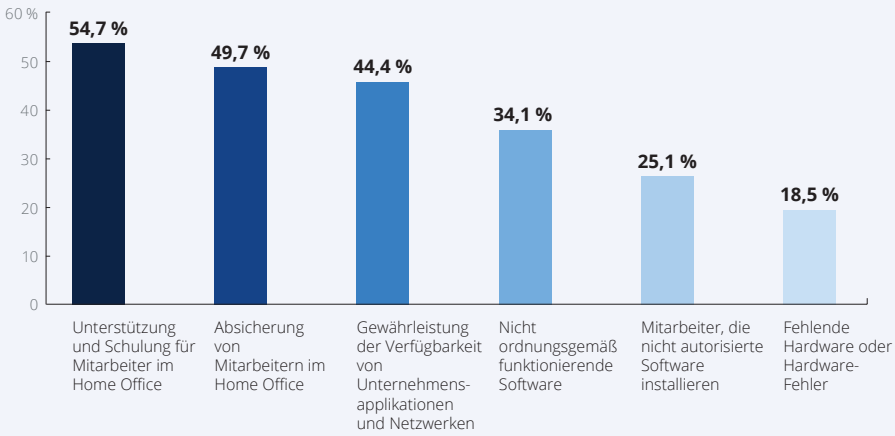
Wir wollten wissen, wie gut sich IT-Teams in dieser Situation bewährten, d. h. an welcher Stelle ihnen der Wechsel in Remote-Umgebungen gelungen ist und wo noch Verbesserungsbedarf besteht. Dazu haben wir unseren ersten Acronis Cyber Readiness Report ausgearbeitet. Für diesen Bericht führten wir im Juni und Juli 2020 eine Umfrage unter 3.400 Unternehmen und Mitarbeitern im Home Office durch. Gefragt wurde nach ihren Erfahrungen mit den Bedrohungen, Herausforderungen und Trends seit dem Wechsel ins Home Office. Die Ergebnisse sind alarmierend:

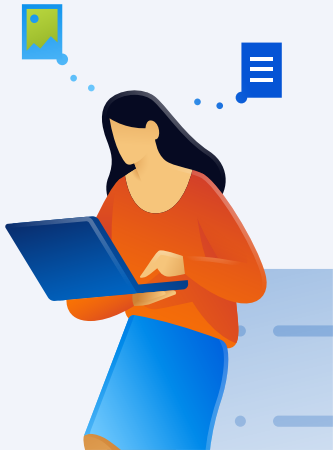
- Beinahe die Hälfte aller IT-Manager hatten Schwierigkeiten bei der Schulung und Absicherung ihrer Mitarbeiter im Home Office.
- 31 % der weltweiten Unternehmen werden mindestens einmal am Tag von Cyberkriminellen angegriffen. Die häufigsten Angriffstypen waren Phishing-Versuche, DDoS-Angriffe sowie Attacken auf Videokonferenzen.
- 92 % der Unternehmen aus aller Welt mussten neue Technologien implementieren, um den Wechsel ins Home Office zu bewerkstelligen. Aus diesem Grund stiegen die IT-Kosten bei 72 % der Unternehmen im Zuge der Pandemie.
- Trotz gestiegener Ausgaben für Technik sind weiterhin Angriffe erfolgreich, da Unternehmen die Schutzmaßnahmen nicht hoch genug priorisieren.
- 39 % aller Unternehmen meldeten während der Pandemie Angriffe auf Videokonferenzen.

IT-Manager bereitet die Schulung von Mitarbeitern zur Arbeit im Home Office die größten Probleme

Frage 1: Mit welchen Herausforderungen waren Sie während der Pandemie konfrontiert in Bezug auf die Verwaltung der steigenden Anzahl an Mitarbeitern im Home Office?

Acronis Cyber Readiness Report 2020





Mehr Zoom-Angriffe durch Coronavirus

Seit Beginn der COVID-19-Pandemie verzeichnet die Videokonferenzplattform Zoom einen enormen Zuwachs der Benutzerzahlen. Dies rief nicht nur Cyberkriminelle auf den Plan; auch Sicherheitsexperten machten sich daran, den Zoom-Code auf Schwachstellen zu überprüfen und Datenschutzbedenken zu melden.

Beispielsweise berichtete Vice.com von zwei Zero-Day-Schwachstellen – also dem Anbieter unbekannte und daher ungepatchte Sicherheitslücken – im Dark Web-Markt: eine für Windows und eine weitere für macOS. Der Zoom Windows RCE-Exploit (Remote Code Execution, Remote-Code-Ausführung) stand für 500.000 US-Dollar zum Verkauf.

Zudem wurde Zoom zum Ziel einer Phishing-Kampagne, die es auf Service-Anmeldedaten abgesehen hatte. In mehr als 50.000 Postfächer gingen Phishing-E-Mails ein, die sich an Microsoft 365-Benutzer richteten. Die Empfänger erhielten eine gefälschte Einladung zu einem Zoom-Gespräch mit der Personalabteilung, bei dem es um eine Leistungsbeurteilung gehen sollte. Dieses Thema soll beim Opfer Anspannung auslösen und kann die übliche Vorsicht beim Klicken auf Links außer Kraft setzen. In Verbindung mit Credential Stuffing-Attacken (bei denen Angreifer ausprobieren, ob der Benutzer das gleiche Kennwort bei mehreren Diensten genutzt hat) führten solche Phishing-Angriffe dazu, dass die Anmeldedaten von mehr als 500.000 Benutzern in Untergrundforen verfügbar sind.

Viele Zoom-Videokonferenzen waren nicht per Kennwort geschützt, was für Cyberkriminelle ebenfalls eine Einladung war. Manche Menschen probierten so lange mögliche ID-Nummern aus, bis sie ein laufendes Meeting fanden. Dann schalteten sie sich in das Gespräch ein und störten die Teilnehmer durch Videos, laute Musik oder unerwünschte Inhalte. Diese als „Zoom-Bombing“ bezeichneten Attacken führten dazu, dass zahlreiche Schulen ihren Fernunterricht einstellten.

Nicht nur Zoom: Auch Microsoft 365-Benutzer betroffen

Natürlich war Zoom nicht das einzige Zusammenarbeitstool im Visier der Angreifer. Ähnliche Angriffe erfolgten auch auf Microsoft Teams und Webex. Beispielsweise wurden innerhalb einer Woche bis zu 50.000 Benutzer von Microsoft 365 angegriffen, wobei die Phishing-E-Mails die Opfer mit gefälschten Microsoft Teams-Benachrichtigungen zu einer gefälschten Microsoft 365-Anmeldeseite weiterleiteten.

Microsoft-Dateifreigabe-Services wie Sway, SharePoint und OneNote wurden mehrfach mit kleinen Phishing-Kampagnen angegriffen, die sich gegen Finanzdienstleister, Anwaltskanzleien und Immobiliengruppen richteten. Ein Angriff, der aufgrund der Ausnutzung von Sway als „PerSwaysion" bezeichnet wurde, erfolgt in drei Schritten: Zuerst werden Phishing-E-Mails mit böswilligen PDF-Anhängen versendet, die sich als Microsoft 365-Benachrichtigung zur Dateifreigabe mit einem „Jetzt lesen"-Hyperlink ausgeben. Ein Klick auf den Link öffnet ein weiteres Köderdokument in einem Microsoft-Dateifreigabedienst (meist Sway) mit einem weiteren „Jetzt lesen"-Link, der die Opfer zu einer gefälschten Microsoft-Anmeldeseite zur Eingabe ihrer Benutzerdaten führt.

Fehlende Sicherheit für Mitarbeiter im Home Office

Nachdem viele Menschen nun von Zuhause mit ihren eigenen Computern arbeiten, lassen sich die Sicherheitsprobleme kaum noch kontrollieren. Zum einen fehlt diesen privaten Rechnern häufig effektive Cyber Protection, zum anderen installieren viele Benutzer nicht regelmäßig die neuesten Sicherheits-Patches für ihr Betriebssystem sowie typische Drittherstellers-Software. Dadurch sind die Computer anfällig für Sicherheitskompromittierungen.

Hinzu kommt, dass private Rechner meist nicht von der IT-Abteilung verwaltet und ohne Unternehmensrichtlinien betrieben werden.

Die Schließung dieser Schwachstellen und Beseitigung der Probleme bei der Patch-Verwaltung am Edge bereitete Administratoren und Technikern, die kleinen Unternehmen IT-Support leisten, viel Kopfzerbrechen.

Zusätzlich sind Heimnetzwerke häufig mit ungeschützten Geräten (z. B. denen der Kinder oder anderer Familienmitglieder) verbunden. Auch der Router kann ein Problem darstellen, wenn er veraltet ist und von Angreifern übernommen werden kann, um bestimmten Datenverkehr umzuleiten.

3. Cyberkriminelle konzentrieren sich auf MSPs

Da viele kleine und mittelständische Unternehmen von Managed Service Providern (MSPs) unterstützt werden, wurden viele MSPs mit Cyber-Angriffen attackiert. Die Logik ist simpel: Anstatt 100 unterschiedliche Unternehmen zu kompromittieren, müssen die Kriminellen lediglich einen MSP hacken, um Zugriff auf 100 Kunden zu erhalten. Angriffe im Jahr 2020 zeigten, dass MSPs mit verschiedensten Techniken kompromittiert werden können, wobei unzureichend konfigurierte Remote-Zugriff-Software einer der Hauptvektoren ist. Cyberkriminelle nutzten Schwachstellen sowie fehlende Zwei-Faktor-Authentifizierung aus und setzten auf Phishing, um Zugriff auf die MSP-Verwaltungswerkzeuge und letztendlich die Client-Computer zu erhalten.

Beispielsweise meldete DXC Technology, ein weltweiter Anbieter von IT-Services und Lösungen, einen Ransomware-Angriff auf seine Systeme, der über das Tochterunternehmen Xchanging erfolgt war. Xchanging unterstützt zwar in erster Linie Unternehmen in der Versicherungsbranche, doch die Kundenliste umfasst auch Firmen aus anderen Sektoren: Finanzdienstleister, Luft- und Raumfahrt, Verteidigung, Automobilhersteller, Bildungswesen, Konsumgüter, Gesundheitswesen und Fertigung.

Ein weiteres Beispiel war der kanadische MSP Pivot Technology Solutions, der einen Cyber-Angriff auf seine IT-Infrastruktur meldete. Die Datenkompromittierung bei Pivot Technology ließ sich auf einen Ransomware-Angriff zurückführen und betrifft möglicherweise auch die personenbezogenen Informationen der Kunden. Dieses Szenario ist typisch für 2020 – und wir rechnen mit einer wachsenden Zahl solcher Vorfälle.

4. Ransomware ist immer noch die Bedrohung Nr. 1

2020 war ganz klar ein Jahr der Ransomware mit mehr Angriffen, größeren Verlusten und neuen Erpressungstechniken, die von Cyberkriminellen implementiert wurden. Praktisch jede Woche werden neue schwerwiegende Fälle bekannt. Laut einem Bericht von Coalition, einem der größten Anbieter von Cyberversicherungen in Nordamerika, machten Ransomware-Vorfälle 41 % der Cyberversicherungsfälle in der ersten Hälfte 2020 aus. „Ransomware beschränkt sich nicht auf bestimmte Sektoren. Wir haben eine Zunahme von Lösegeldangriffen in fast allen Branchen erlebt, in denen wir aktiv sind", so Coalition. Dies können wir bei Acronis bestätigen.

In den nächsten Abschnitten dieses Berichts finden Sie detaillierte Statistiken unserer Cyber Protection Operation Center. Hier an dieser Stelle geben wir lediglich einen allgemeinen Überblick über die bedrohliche Entwicklung.

Große Ziele bringen große Lösegelder

Am 18. Juli wurde der größte argentinische Telekommunikationsanbieter von einem Ransomware-Angriff getroffen (vermutlich durchgeführt von der Sodinokibi-Gruppe), der ein Lösegeld von 7,5 Millionen US-Dollar forderte. Wie für solche Angreifer typisch, die eine schnelle Entscheidung erzwingen wollen, drohten sie mit einer Verdoppelung der Lösegeldforderung, wenn die Bezahlung nicht innerhalb von 48 Stunden erfolgte. Die Ransomware soll mehr als 18.000 Workstations infiziert haben, darunter Terminals mit äußerst vertraulichen Daten.

Garmin, einer der weltweit größten Anbieter von Wearable-Geräten, bestätigte Berichte über einen schwerwiegenden Ausfall nach einem Angriff mit der Ransomware WastedLocker am 24. Juli.

Aufgrund dieses Zwischenfalls musste Garmin den Betrieb im Contact Center, Garmin Connect sowie die Produktion in Taiwan stilllegen. Mit einem Jahresumsatz von geschätzt 4 Milliarden US-Dollar ist Garmin in jedem Fall ein lohnenswertes Ziel. Die geforderte Lösegeldsumme soll bei 10 Millionen US-Dollar gelegen haben. Bei anderen aktuellen WastedLocker-Angriffen sollen die Forderungen zwischen 500.000 und mehreren Millionen US-Dollar gelegen haben.

Die Liste der Opfer hoher Lösegelderpressungen ist lang. Im Februar 2020 veröffentlichte das FBI eine Schätzung der Profite einiger Ransomware-Gruppen. Demnach sollen Gruppen wie Ryuk im Jahr 2019 monatlich etwa 3 Millionen US-Dollar erpresst haben. Angesichts derartiger Profite ist nicht damit zu rechnen, dass diese Aktivitäten in absehbarer Zeit zurückgehen.

Hinzu kommt, dass aktuelle Ransomware-Familien nicht nur Lösegeld für die Entschlüsselung der Daten verlangen, sondern auch dafür, die vertraulichen Daten nicht zu veröffentlichen. Dies steigert die Wahrscheinlichkeit, dass die Opfer wirklich zahlen.

Lösegeldforderung für Nichtveröffentlichung

Die Ransomware-Gruppe REvil/Sodinokibi gab am 14. August bekannt, dass sie das im US-Bundesstaat Kentucky ansässige Unternehmen Brown-Forman kompromittiert hatte, Mutterunternehmen von Whiskey-Marken wie Jack Daniels, Old Forester, The Glendronach sowie weiterer Spirituosen und Weine. Brown-Forman fuhr im Jahr 2020 einen Bruttogewinn von mehr als 2 Milliarden US-Dollar und einen Nettogewinn von 872 Millionen ein, was das Unternehmen zu einem lukrativen Ziel für Ransomware-Betreiber macht.

Die REvil-Gruppe behauptete, an 1 TB an Daten gelangt zu sein, zu denen vertrauliche Mitarbeiterinformationen, Finanzdaten, interne Kommunikation sowie Unternehmensverträge zählen. Auf der Leak-Website veröffentlichte Bilder deuten darauf hin, dass die erbeuteten Daten mindestens bis ins Jahr 2009 zurückreichen.

Canon, ein multinationaler Anbieter für optische und bildgebende Produkte, wurde erfolgreich mit der Ransomware Maze angegriffen. Betroffen waren das E-Mail-System, Microsoft Teams, die US-amerikanische Website sowie weitere interne Applikationen. Die Betreiber der Ransomware gaben an, dass sie mehr als 10 TB an Daten von Canon, inklusive privater Datenbanken, erbeutet hatten. In einer internen Nachricht an die Mitarbeiter bestätigte Canon den Angriff.

CWT, einer der weltweit größten Anbieter für Reisen und Event Management, wurde mit der Ransomware Ragnar Locker angegriffen, wobei die Angreifer 2 TB mit vertraulichen Unternehmensdaten erbeutet und dabei mehr als 30.000 Systeme kompromittiert haben sollen. Während die Angreifer ursprünglich 10 Millionen US-Dollar für die Rückgabe der gestohlenen Daten verlangt hatten, konnte CWT ein Lösegeld von 414 Bitcoin aushandeln – die zum damaligen Zeitpunkt mehr als 4 Millionen US-Dollar Wert waren.

Conti ist ein neuer Ransomware-as-a-Service (RaaS) und Nachfolger der berüchtigten Ryuk-Variante. Seine Betreiber erstellten im Rahmen ihrer Erpressungen eine Datenleck-Website, um die Opfer zur Lösegeldzahlung zu erpressen. Conti war monatelang lang aktiv, doch erst vor Kurzem stellten die Cyberkriminellen eine Datenleck-Website ins Netz, auf der sie damit drohen, die gestohlenen Daten ihrer Opfer zu veröffentlichen, sofern das geforderte Lösegeld nicht bezahlt würde. „Conti.News“ führt derzeit 112 Opfer auf, darunter auch große und bekannte Unternehmen.

Insgesamt haben etwa 20 verschiedene Ransomware-Gruppen spezielle Webseiten für Datenlecks erstellt, die über das Tor-Netzwerk erreichbar sind. Dabei wurden die Daten von mehr als 700 Unternehmen veröffentlicht, von denen 37 % aus Infektionen mit der Ransomware Maze stammten, gefolgt von Conti mit 15 % und Sodinokibi mit 12 %.

Eine Folge dieser Datenschutzverletzungen können Reputationsverlust, weitere Angriffe und Geldstrafen sein. Hinzu kommt, dass die Kompromittierung von Kundendaten gemäß Datenschutzbestimmungen wie der DSGVO oder CCPA Bußgelder nach sich ziehen können. Zudem kann eine Lösegeldzahlung vom US-amerikanischen OFAC (Office of Foreign Assets Control, Amt zur Kontrolle von Auslandsvermögen) bestraft werden.

5. Einfache Backup- und Sicherheitsfunktionen genügen nicht mehr

Seit 2016 haben wir vorhergesagt, dass Ransomware auch Backup-Lösungen angreifen wird. Hintergrund für diese Annahme war, dass Initiativen wie No More Ransom, deren Mitglied Acronis seit 2017 ist, Benutzer und Unternehmen dazu aufruft, keine Lösegelder mehr zu zahlen. Stattdessen propagiert die Initiative ausreichenden Ransomware-Schutz für die Computer. Wenn Sie über ein Backup verfügen, müssen Sie kein Lösegeld bezahlen, sondern können jederzeit eine Wiederherstellung starten. Das war der Grundgedanke, doch die Cyberkriminellen fanden schnell eine neue Methode. Ab 2017 begannen praktisch alle Ransomware-Varianten, Windows-Volume-Schattenkopien zu löschen oder zu deaktivieren und versuchten, herkömmliche Backup-Lösungen abzuschalten. Da viele dieser Backup-Lösungen nur über sehr grundlegende (oder gar keine) Selbstschutzfunktionen verfügen, war das nicht schwer. Der von NioGuard Security Lab (Mitglied bei AMTSO) durchgeführte Test ist ein gutes Beispiel dieser bedrohlichen Situation.

Im Folgenden stellen wir zwei aktuelle Ransomware-Exemplare genauer vor.

RANSOMWARE CONTI:

- Die durchschnittliche Lösegeldforderung für diese Ransomware liegt bei weniger als 100.000 US-Dollar.
- Nutzt den Neustart-Manager von Windows zum Schließen aller offenen oder nicht gespeicherten Dateien vor der Verschlüsselung.
- Enthält mehr als 250 Entschlüsselungsroutinen für Zeichenfolgen sowie eine Liste von 150 zu beendenden Services.
- Führt eine schnelle Dateiverschlüsselung in 32 simultanen Threads mithilfe der E/A-Abschlussports von Windows durch.
- Folgt dem Trend und hat kürzlich die Datenleck-Website „Conti.News“ online gestellt.

Hinzu kommt, dass die Ransomware Schattenkopien der Dateien löscht und die Größe des Schattenkopie-Speicherplatzes auf den Laufwerken C: bis H: verändert, was ebenfalls zum Verschwinden von Schattenkopien führen kann. Auch Services für SQL, Virenschutz-, Cyber Security- und Backup-Lösungen wie BackupExec und Veeam werden angehalten. Die Ransomware versucht auch, Acronis Cyber Protect zu deaktivieren, scheitert jedoch an unseren Selbstschutzfunktionen. Zu den ca. 150 Services gehören unter anderem:

Acronis VSS Provider	BackupExecRPCService	VeeamDeploySvc
Veeam Backup Catalog Data Service	BackupExecVSSProvider	VeeamEnterpriseManagerSvc
AcronisAgent	EPSecurityService	VeeamMountSvc
AcrSch2Svc	EPUpdateService	VeeamNFSSvc
Antivirus	mozyprobackup	VeeamRESTSvc
BackupExecAgentAccelerator	VeeamBackupSvc	VeeamTransportSvc
BackupExecAgentBrowser	VeeamBrokerSvc	VeeamHvIntegrationSvc
BackupExecDeviceMediaService	VeeamCatalogSvc	Zoolz 2 Service
BackupExecJobEngine	VeeamCloudSvc	AVP
BackupExecManagementService	VeeamDeploymentService	

RANSOMWARE NETWALKER:

Ein weiteres Beispiel ist die Ransomware NetWalker, die zum ersten Mal im August 2019 „in the wild“ gesichtet wurde. Sie nutzt das RaaS-Modell und greift sowohl Unternehmen als auch einzelne Benutzer an. Seit März 2020 haben die Betreiber auf diese Weise rund 25 Millionen US-Dollar an Lösegeldern erpresst. Das auffälligste Merkmal der neuesten NetWalker-Version ist der stark verschleierte PowerShell-Loader, der die Ransomware auf einem infizierten System startet. Die Nutzung von PowerShell-Skripts bzw. allgemein der Missbrauch vorinstallierter Tools mit Living-of-the-Land-Taktiken für opportunistische Vorgehensweisen ist bei Cyberkriminellen weiterhin sehr beliebt.

Ebenso wie andere Ransomware-Varianten auch löscht NetWalker die Windows-Schattenkopien der Dateien.

```
Get-Wmiobject Win32_Shadowcopy | ForEach-Object {$_.Delete();} | Out-Null
```

Außerdem versucht NetWalker, mit folgenden Zeichenfolgen beginnende Backup-Services zu anzuhalten, um eine Wiederherstellung zu verhindern:

veeam*	ShadowProtectSvc	StorageCraft ImageManager
backup*	AcronisAgent	acrsch2svc*
backup	AcrSch2Svc	

Teil 2

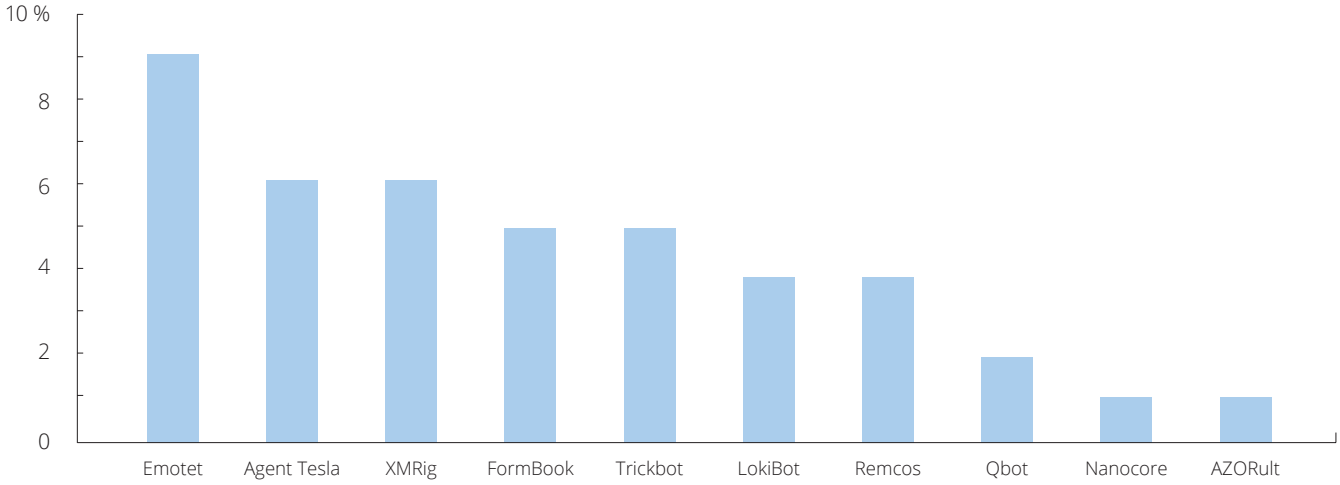
Allgemeine Malware-Bedrohungen

Im 3. Quartal 2020 verzeichneten durchschnittlich 11 % unserer Kunden mindestens einen erfolgreich abgewehrten Malware-Angriff. Die Zahl ging leicht auf die Normalwerte seit Beginn der Pandemie zurück. Im Juli lag sie immer noch bei 14,7 %, im August bei 10,1 %, im September bei 8,9 % und im Oktober bei 6,7 %.

Die Länder mit den meisten Kunden, die im 3. Quartal 2020 Malware-Angriffe entdeckt hatten, waren die USA mit 27,9 %, gefolgt von Deutschland mit 16,7 % und Großbritannien mit 6,1 %.

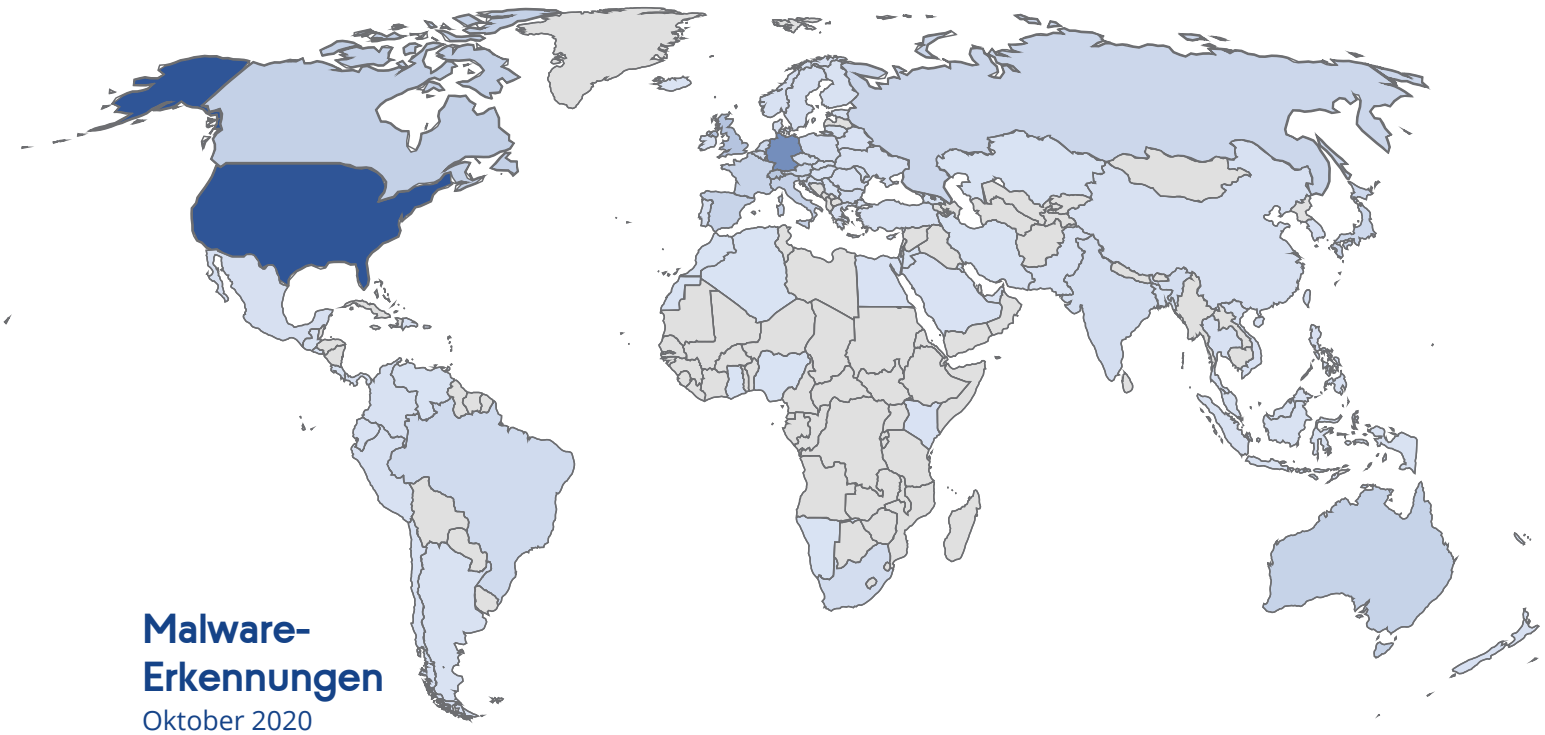
Das unabhängige Malware-Testlabor AV-TEST verzeichnete im 3. Quartal 2020 pro Tag 400.000 neue Malware-Varianten, was deutlich zeigt, dass Cyberkriminelle ihre Prozesse automatisieren und eine Flut neuer Malware-Bedrohungen generieren. Die meisten dieser Bedrohungen werden jedoch nur für einige wenige Angriffe innerhalb eines kurzen Zeitraums verwendet. Von den von uns entdeckten Varianten wurden 19 % nur einmal beobachtet. Die durchschnittliche Lebensdauer eines böswilligen Exemplars lag bei 3,4 Tagen, bevor es auf Nimmerwiedersehen verschwand.

Diese 10 häufigsten Malware-Familien beobachteten und verfolgten wir im Jahr 2020:



Anteil der weltweiten monatlichen Erkennungen pro Land

LAND	OKTOBER 2020	SEPTEMBER 2020	AUGUST 2020	JULI 2020
USA	27,5 %	27,9 %	29,3 %	16,4 %
Deutschland	18,4 %	16,7 %	16,8 %	4,3 %
Schweiz	7,2 %	5,4 %	3,6 %	3,2 %
Großbritannien	5,9 %	6,1 %	6,4 %	4,5 %
Kanada	3,0 %	3,6 %	3,6 %	1,5 %
Frankreich	3,0 %	2,9 %	3,3 %	2,3 %
Italien	3,0 %	3,2 %	3,3 %	1,7 %
Australien	3,0 %	3,3 %	3,1 %	2,0 %
Spanien	2,6 %	3,0 %	2,8 %	4,2 %
Japan	2,0 %	2,3 %	3,2 %	15,7 %



Malware-Erkennungen

Oktober 2020

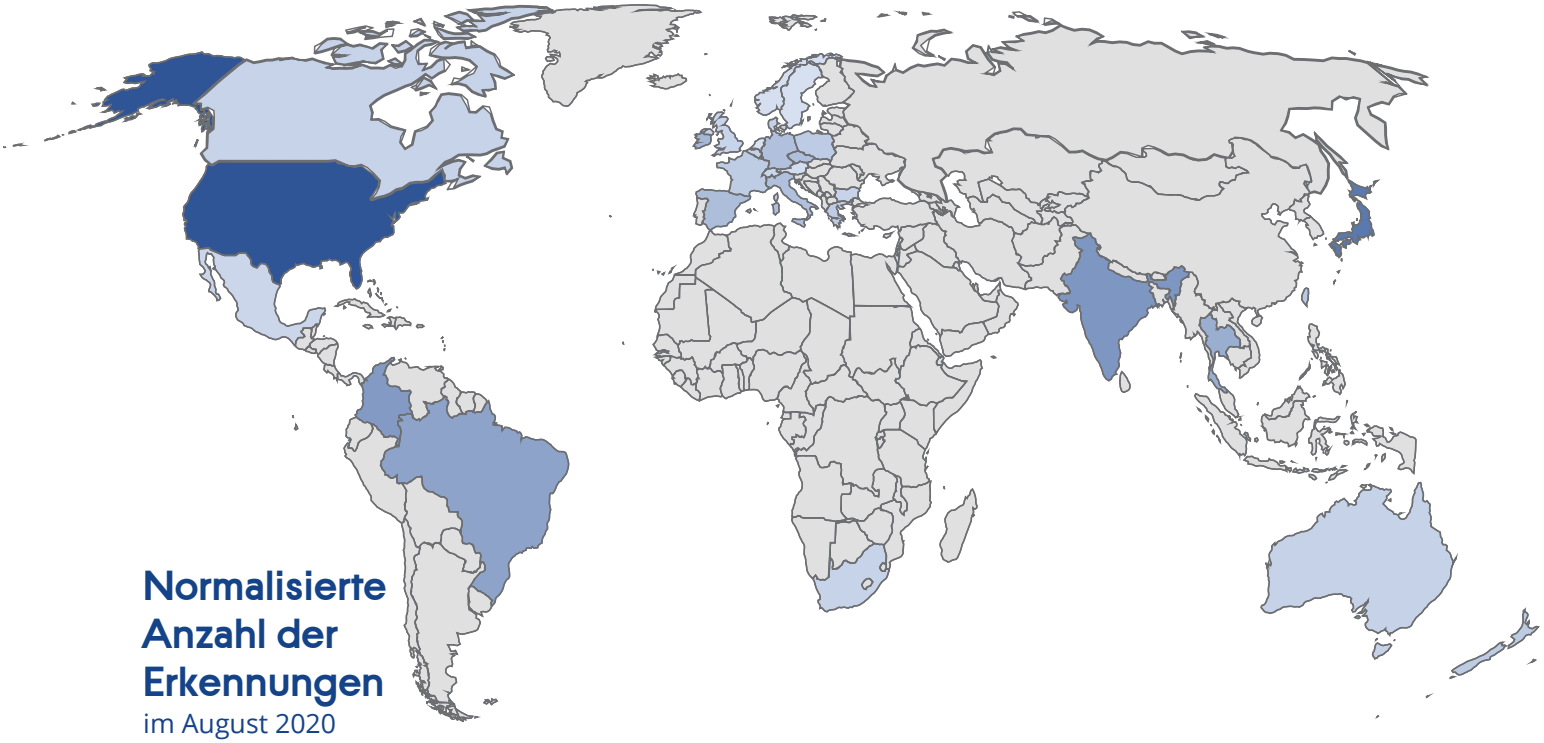
Anteil

0 % 0,27 %

Wenn wir die Zahl der Erkennungen nach aktiven Kunden pro Land normalisieren, erhalten wir eine etwas andere Verteilung. Die folgende Tabelle zeigt die Zahl der Erkennungen pro 1.000 Kunden pro Land. Dies zeigt deutlich, dass Cyberbedrohungen ein weltweites Phänomen sind.

RANG	LAND	MALWARE-ERKENNUNGEN pro 1.000 Kunden im August
1	USA	2.059
2	Japan	1.571
3	Indien	1.168
4	Kolumbien	1.123
5	Brasilien	994
6	Thailand	856
7	Irland	729
8	Spanien	634
9	Tschechische Republik	611
10	Deutschland	601
11	Italien	589

RANG	LAND	MALWARE-ERKENNUNGEN pro 1.000 Kunden im August
12	Hongkong	518
13	Taiwan	480
14	Neuseeland	462
15	Polen	453
16	Frankreich	444
17	Griechenland	437
18	Dänemark	375
19	Australien	361
20	Belgien	358
21	Südafrika	351
22	Bulgarien	351
23	Kanada	347
24	Großbritannien	329
25	Schweiz	311



Normalisierte Anzahl der Erkennungen
im August 2020

Anzahl der Erkennungen pro 1.000 Kunden

131 2.059

Ransomware-Bedrohungen

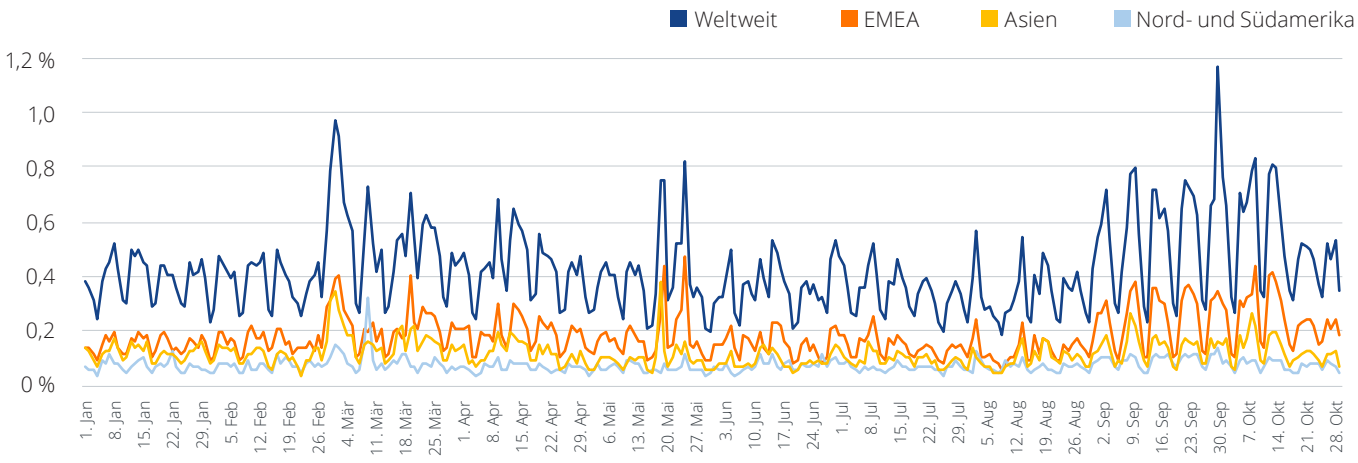
Wie bereits im Abschnitt zu den wichtigsten Trends erwähnt, ist Ransomware weiterhin die Cyberbedrohung Nr. 1 für Unternehmen. Obwohl wir bereits seit 2017 Ransomware beobachten, als die erste Version von Acronis Active Protection erschien, konzentrieren wir uns in diesem Abschnitt auf Daten vom 1. Januar bis 31. Oktober 2020.

Diese 10 häufigsten Ransomware-Familien beobachteten und verfolgten wir im Jahr 2020. Wichtig ist dabei, dass einige Gruppen einen weit gefächerten Ansatz verfolgen, um so viele Benutzer wie möglich zu infizieren, während sich andere Gruppen auf wertvolle Ziele konzentrieren, bei denen sie mit wenigen Infektionen hohe Profite erreichen können. Aus diesem Grund ist die bloße Zahl von Bedrohungserkennungen kein Hinweis darauf, wie gefährlich eine Bedrohung ist.

In den letzten neun Monaten tauchten nach unseren Beobachtungen etwa 50 neue Ransomware-Familien auf. Einige gehören zu kleineren Gruppen, die sich auf Privatanwender konzentrieren, doch neue Gruppe wie Avaddon, Mount Locker und Suncrypt haben es auf die profitableren Unternehmen abgesehen. Eine wachsende Zahl dieser Gruppen ist im Ransomware-as-a-Service-Geschäft aktiv und agiert als Re-Distributoren bereits etablierter Bedrohungen. Dies steigert die Verbreitung häufiger Ransomware-Bedrohungen nur noch weiter.

Tägliche Ransomware-Erkennungen

In diesem Jahr beobachteten wir eine deutliche weltweite Zunahme zu Beginn des COVID-19-Lockdowns im März. Seither bleiben die Ransomware-Aktivitäten auf einem höheren Niveau als zuvor. Bezüglich der attackierten Sektoren oder geografischen Regionen haben wir festgestellt, dass es keine Ausnahmen gibt – alle Branchen werden von den Angreifern ins Visier genommen. Ab September registrierten wir eine weitere Welle von Ransomware-Angriffen, die sich insbesondere gegen Bildungseinrichtungen und Fertigungsunternehmen in Nordamerika richteten.



Top 10 der Länder: Ransomware-Erkennungen nach Region

Asien:

LAND	Regionale Ransomware-Erkennungen Anteil im 3. Quartal 2020
Japan	17,7 %
Philippinen	13,3 %
Taiwan	9,6 %
China	8,6 %
Indien	7,8 %
Türkei	5,4 %
Iran	5,3 %
Südkorea	3,9 %
Indonesien	3,7 %
Thailand	3,6 %

EMEA:

LAND	Regionale Ransomware-Erkennungen Anteil im 3. Quartal 2020
Deutschland	17,7 %
Frankreich	13,3 %
Italien	9,6 %
Großbritannien	8,6 %
Schweiz	7,8 %
Spanien	5,4 %
Österreich	5,3 %
Niederlande	3,9 %
Belgien	3,7 %
Tschechische Republik	3,6 %

Nord- und Südamerika:

LAND	Regionale Ransomware-Erkennungen Anteil im 3. Quartal 2020
USA	67,3 %
Kanada	15,9 %
Chile	4,7 %
Brasilien	3,0 %
Mexiko	2,7 %
Kolumbien	1,7 %
Peru	1,0 %
Argentinien	0,8 %
Bolivien	0,4 %
Ecuador	0,3 %

Ransomware-Gruppen im Rampenlicht

Die getarnte Ransomware Maze verschlüsselt und exfiltriert Terabytes an privaten Daten bei gezielten Angriffen

Die Ransomware Maze führt mindestens seit Mai 2019 gezielte Angriffe durch und soll für den neuesten Angriff auf Canon am 30. Juli 2020 verantwortlich sein, der zum Ausfall des Cloud Storage-Service image.canon führte. Außerdem behauptet der Maze-Betreiber, im Rahmen dieses Angriffs an 10 TB privater Daten gelangt zu sein. Sie hatten bereits Daten von Xerox und LG veröffentlicht, die bei erfolgreichen Angriffen im Juni 2020 erbeutet wurden, da die Unternehmen die Lösegeldzahlungen verweigert hatten.

- **Verschlüsselt die Daten nicht nur, sondern stielt sie zusätzlich, damit sie veröffentlicht werden können, wenn das Lösegeld nicht gezahlt wird**
- **Canon, Xerox und LG gehören zu den größten Maze-Opfern**
- **Nutzt Techniken zur Verhinderung von Disassemblierung und Debugging**
- **Verschlüsselt nicht Systeme mit russischen Landeseinstellungen**
- **Aufruf von wmic.exe zum Löschen von Schattenkopien ist verschleiert**
- **Sendet eine HTTP-Check-in-Anfrage an den C&C-Server, der sich im Netzwerk „91.218.114.0“ in Moskau (Russland) befindet**
- **Nutzt zur Verbreitung die Hacker-Tools Mimikatz, ProcDump und Cobalt Strike**

Die Ransomware Maze wird typischerweise bei einem gezielten Angriff auf ein Unternehmen übertragen, der mit einer Spearphishing-E-Mail beginnt. Dabei erfolgt der Zugriff über eine kompromittierte RDP- oder VDI-Verbindung (die Anmeldedaten stammen üblicherweise aus dem Dark Web) und Schwachstellen in VPNs (virtuelle private Netzwerke) werden ausgenutzt.

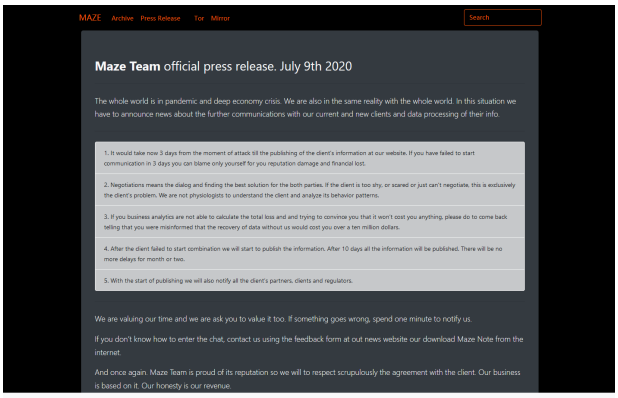
Sobald der Maze-Betreiber Zugriff auf das interne Netzwerk des Unternehmens erlangt, führt die Ransomware Mimikatz und Procdump aus, um Kennwörter aus dem Arbeitsspeicher zu erfassen und mit dem Cobalt Strike-Red-Teaming-Tool in den Aufklärungsmodus zu wechseln.

Maze nutzt Techniken zur Verhindern der Disassemblierung, um die Code-Analyse in einem Disassembler zu erschweren.

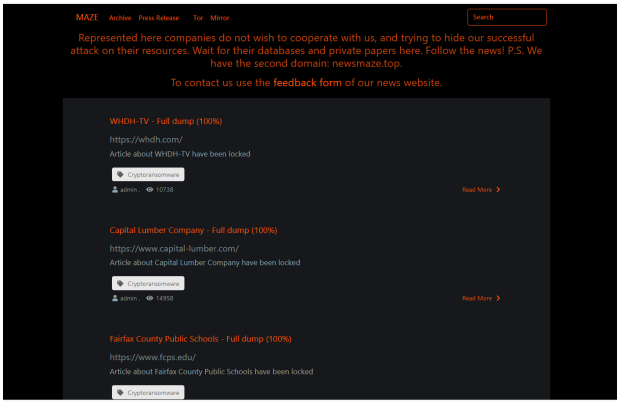
Folgende Verschleierungstechniken werden verwendet:

1. **Bedingte Sprünge, die an die gleiche Stelle weiterleiten und absolute Sprünge ersetzen**
2. **Nach Aufrufen erfolgt ein Push der Rückadresse zum Stack, anschließend erfolgt der Sprung zur Aufrufadresse**

Hinzu kommt, dass Maze erkennen kann, wenn ein Debugging seines Codes stattfindet. Die Ransomware überprüft über das Flag „BeingDebugged" in der PEB-Struktur, ob der Prozess unter einem Debugger ausgeführt wird. In diesem Fall geht der Code in eine unendliche Schleife und führt keine Verschlüsslung durch. Zudem beendet Maze die Prozesse der Malware-Analyse- und Office-Tools anhand der Hash-Werte der Prozessnamen.



Die Ransomware Maze geht ähnlich vor wie andere aktuelle Ransomware-Familien (z. B. WastedLocker, NetWalker und REvil) und verschlüsselt die Daten nicht nur, sondern exfiltriert sie auch. Die Malware nutzt das Hilfsprogramm 7zip, um die erfassten



Daten zu packen und die Archive mithilfe des WinSCP-Clients zum FTP-Server des Angreifers zu übertragen. In einigen Fällen wurde gemeldet, dass die exfiltrierten Daten ebenfalls Base64-codiert wurden.

Dadurch wird Maze zu einer der gefährlichsten Ransomware-Familien, die wir im Jahr 2020 entdeckt haben.

Die Ransomware DarkSide greift keine Krankenhäuser, Schulen und Behörden an

Eine neue Ransomware-Variante ist DarkSide. Die Angriffe mit dieser Malware begannen im August 2020 und wurden angeblich von ehemaligen Partnern anderer Ransomware-Kampagnen durchgeführt, die im Erpressungsgeschäft aktiv waren und beschlossen, ihren eigenen Code zu entwickeln. Bekannt gewordene Zwischenfälle legen nahe, dass die Lösegeldforderungen zwischen 200.000 und 2.000.000 US-Dollar liegen. Ebenso wie andere Ransomware, die für gezielte Angriffe eingesetzt wird, verschlüsselt DarkSide die Benutzerdaten nicht nur, sondern exfiltriert sie auch von den kompromittierten Servern.

Anders als die Ransomware Maze, die den Schulbezirk Newhall (Kalifornien, USA) und Schulen in Fairfax County (Virginia, USA) erfolgreich angriffen, verfügt DarkSide über einen Verhaltenskodex, der Angriffe auf Krankenhäuser, Schulen und Behörden verbietet.

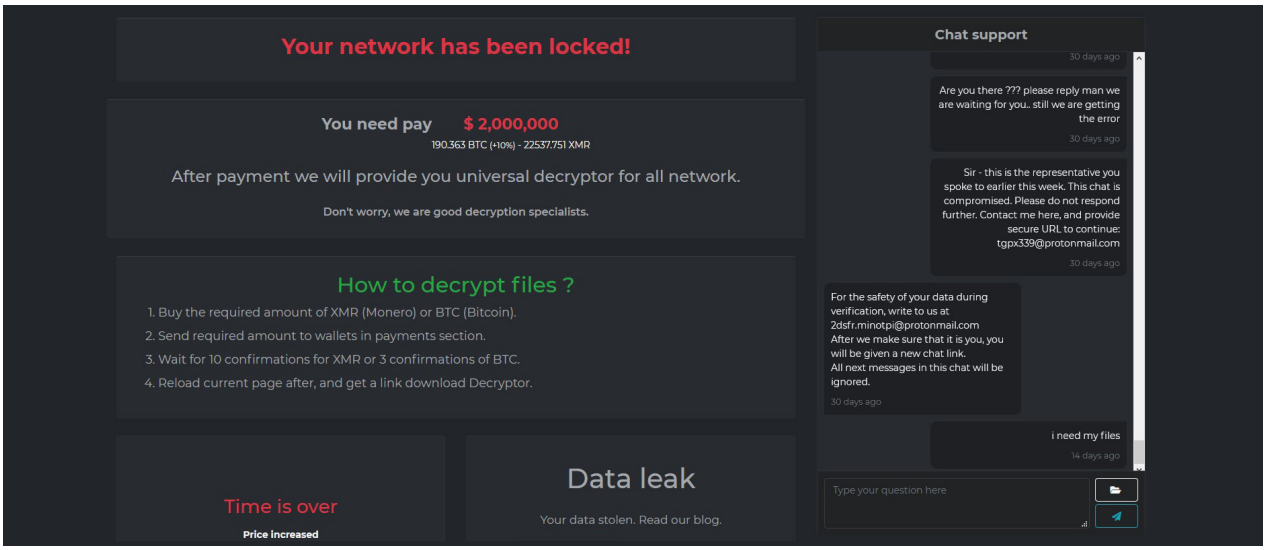
- **Entdeckt im August 2020**
- **Greift lediglich englischsprachige Länder an und meidet frühere Sowjetrepubliken**
- **Greift keine Krankenhäuser, Hospize, Schulen, Universitäten, gemeinnützige Organisationen oder Behörden an**
- **Nutzt Salsa20 mit individueller Matrix und RSA-1024-Verschlüsselungsalgorithmen**
- **Lösegeldzahlungen reichen von 200.000 bis 2.000.000 US-Dollar**

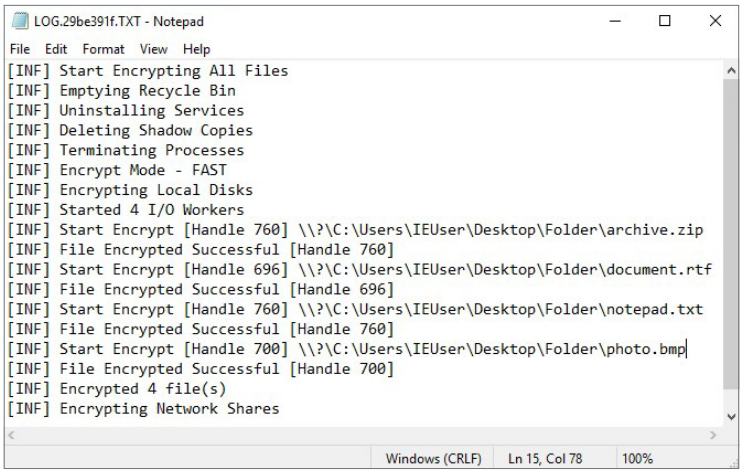
Die Ransomware leert den Papierkorb, ohne dazu die Funktion „SHEmptyRecycleBinA()" zu nutzen, um eine Entdeckung zu vermeiden. Stattdessen werden Dateien und Ordner entfernt, die nach und nach in den Papierkorb verschoben werden.

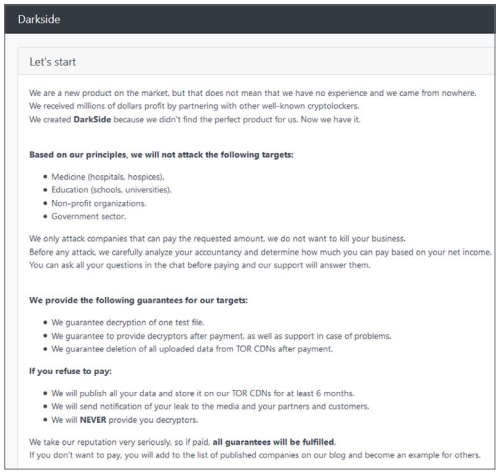
DarkSide deinstalliert die folgenden Services, die zu Sicherheits- und Backup-Lösungen gehören:

Sobald der Volume Shadow Copy Service (VSS) deinstalliert ist, löscht die Ransomware die Schattenkopien, indem sie ein verschleiertes PowerShell-Skript ausführt. DarkSide gibt auch einen Schlüssel an, der auf der ersten Website eingegeben werden muss. Der Schlüssel gilt nicht individuell für den Benutzer, sondern scheint pro Variante zu gelten, da er in der ausführbaren Datei festcodiert und verschlüsselt ist.

Die Schlussfolgerung ist hier die gleiche: Selbst wenig komplexe neue Ransomware-Familien greifen standardmäßig Backups an. Leider ist das der neue Normalzustand.







Böswillige Websites

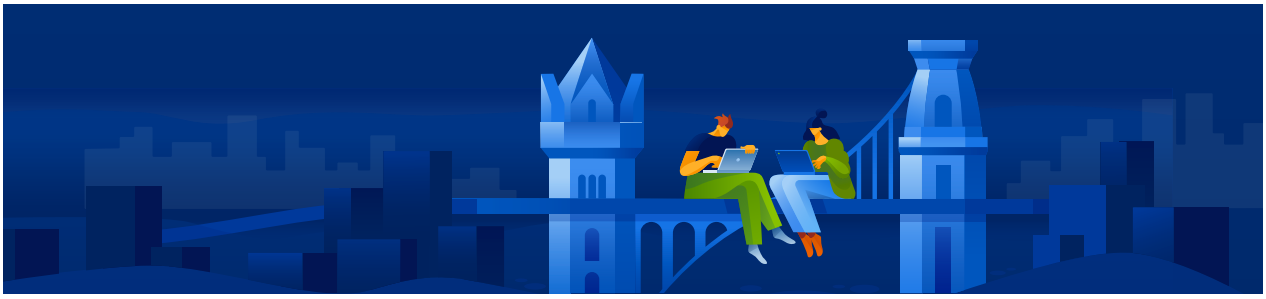
Während der Pandemie erlebten wir eine Zunahme an Phishing-Angriffen – insbesondere gegen Zusammenarbeitstools und Datei-freigabedienste, die seit dem Wechsel ins Home Office verstärkt genutzt werden. Nach einem ersten Anstieg im März gingen diese Attacken wieder zurück. Scheinbar haben einige Gruppen von Cyberkriminellen sich wieder böswilligen Anhängen zugewandt. Selbst die berüchtigte Emotet-Gruppe meldete sich im Juli nach einer fünfmonatigen Pause zurück und verteilte wieder schädliche Office-Dokumente.

MONAT	ANTEIL DER BENUTZER, die böswillige URLs angeklickt haben
Juni	5,5 %
Juli	5,1 %
August	2,3 %
September	2,7 %
Oktober	3,4 %

Im 3. Quartal lag der größte Anteil blockierter URLs in den USA bei 16,4 %, gefolgt von Deutschland mit 14,1 % und Tschechien mit 10,4 %. Dabei waren 51 % der blockierten URLs mit HTTPS verschlüsselt, was ihre Filterung im Netzwerk erschwert. Wir haben auch beobachtet, dass mehr Gruppen per Phishing an 2FA-Token gelangen und sie sofort für skriptgesteuerte Anmeldungen missbrauchen. Um die Erkennung dieser Phishing-Seiten zu erschweren, werden sie häufig bei vertrauenswürdigen Cloud-Service-Providern wie Azure oder Google gehostet. Einige Angreifer fügen sogar eine CAPTCHA-Seite hinzu, die gelöst werden muss, bevor der Benutzer die endgültige Phishing-Seite erreicht. Diese Vorgehensweise kann verhindern, dass automatisierte Scan-Lösungen die Phishing-Website analysieren und blockieren.

Top 20 der Länder mit den meisten blockierten URLs im 3. Quartal

RANG	LAND	ANTEIL DER BLOCKIERTEN URLS IM 3. QUARTAL 2020
1	USA	16,4 %
2	Deutschland	14,1 %
3	Tschechische Republik	10,4 %
4	Spanien	8,3 %
5	Großbritannien	6,7 %
6	China	5,8 %
7	Südafrika	5,2 %
8	Hongkong	3,6 %
9	Italien	3,4 %
10	Australien	2,4 %
11	Frankreich	2,1 %
12	Kanada	2,0 %
13	Peru	1,9 %
14	Norwegen	1,9 %
15	Niederlande	1,8 %
16	Japan	1,6 %
17	Schweiz	1,6 %
18	Bulgarien	0,9 %
19	Singapur	0,8 %
20	Österreich	0,7 %



Teil 3

Schwachstellen im Windows-Betriebssystem und in Windows-Software

1. Drittanbieter-Applikationen sind anfällig und werden auch von Kriminellen genutzt
2. Weltweit am häufigsten ausgenutzte Applikationen

Die Anzahl der entdeckten Schwachstellen und veröffentlichten Patches ist im Jahr 2020 regelrecht explodiert. Das VulnDB-Team von Risk Based Security registrierte in der ersten Hälfte 2020 insgesamt 11.121 Schwachstellen.

Im neuesten Microsoft-Patch vom September meldete das Unternehmen 129 geschlossene Sicherheitsschwachstellen, von denen 23 von Malware ausgenutzt werden konnten, um ganz ohne oder mit geringer Beihilfe von Benutzern die vollständige Kontrolle über Windows-Computer zu erhalten. Dies ist der siebente Monat in Folge, in dem Microsoft Behebungen für mehr als 100 Fehler in den eigenen Produkten veröffentlicht, und der vierte Monat in Folge mit mehr als 120 Fehlerbehebungen.

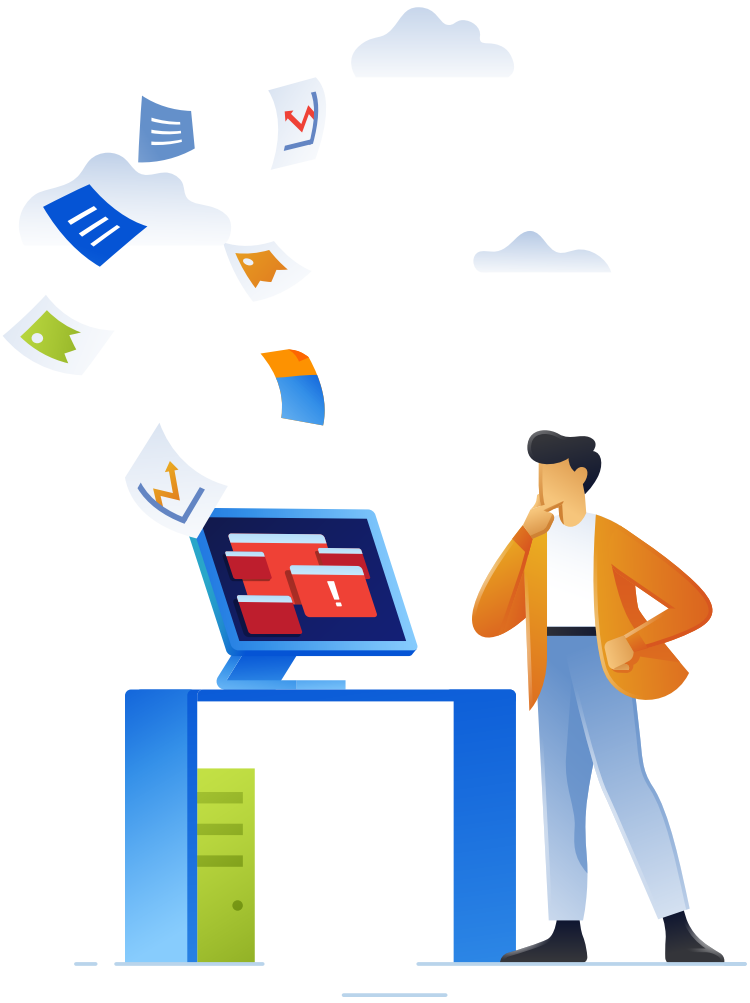
Das Problem ist altbekannt: Selbst wenn ein Anbieter schnell einen Patch veröffentlicht, wird dieser trotzdem nicht überall eingespielt. Beispielsweise galt der potenzielle Missbrauch von CVE-2020-0796 (besser bekannt als SMBGhost) als so gefährlich, dass diese Schwachstelle die seltenste CVSS-Bewertung (Common Vulnerability Scoring System) bekam: eine „perfekte" 10. Innerhalb weniger Tage veröffentlichte Microsoft eine Notfall-Fehlerbehebung. Doch Cyber Security-Firmen auf der ganzen Welt (darunter auch Acronis) haben reale Angriffe auf diese Schwachstelle beobachtet.

Ebenso erhielten CVE-2020-1425 und CVE-2020-1457, zwei RCE-Fehler (Remote-Code Execution), die Bewertung als „kritisch" und „wichtig". Beide Fehler hängen mit der Microsoft Windows Codecs Library zusammen, die Objekte im Arbeitsspeicher verwaltet. Ein Angreifer, der CVE-2020-1425 ausnutzen kann, könnte laut Microsoft „Informationen erlangen, mit denen sich das Benutzersystem weiter kompromittieren lässt". Die erfolgreiche Ausnutzung des zweiten Fehlers könnte Angreifern die Möglichkeit geben, beliebigen Code auf dem Zielcomputer auszuführen. Jeder Fehler erhielt im Microsoft Exploitability Index die Bewertung „Ausnutzung weniger wahrscheinlich".

Einige dieser Schwachstellen werden laut unseren Daten aktiv ausgenutzt: CVE-2020-1020 und CVE-2020-0938. Wie wir am 23. März meldeten, bestätigte Microsoft die aktive Ausnutzung dieser Windows-Schwachstellen, ohne jedoch eine Fehlerbehebung bereitzustellen.

Windows 10-Benutzer ohne installierten Patch laufen Gefahr, dass ein Angreifer Programme installieren, Daten anzeigen oder verändern sowie neue Konten erstellen kann.

Die Windows-Spoofing-Schwachstelle CVE-2020-1464 wird ebenfalls vielfach angegriffen. In Windows besteht ein Fehler, bei dem Dateisignaturen fehlerhaft validiert werden. Ein Angreifer, der diesen Fehler erfolgreich ausnutzen kann, könnte eine böswillige ausführbare Datei mit einer gefälschten Signatur versehen, um jede beliebige Datei zu laden und sie gegenüber dem Betriebssystem als legitim ausgeben. Diese Schwachstelle betrifft alle unterstützten Windows-Versionen und stellt eine erhebliche Gefahr dar, sofern sie nicht gepatcht wird.



Drittanbieter-Applikationen sind anfällig und werden auch von Kriminellen genutzt

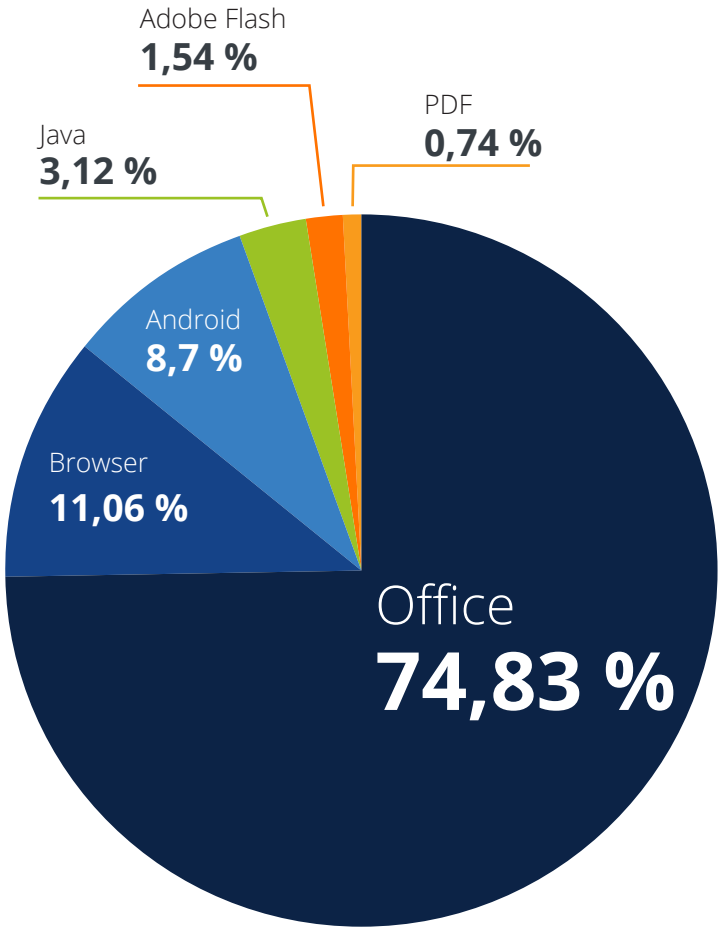
Natürlich ist Microsoft nicht das einzige Unternehmen, dessen Software Schwachstellen aufweist. Im Jahr 2020 haben wir auch die Ausnutzung der folgenden Schwachstellen beobachtet.

Adobe veröffentlicht regelmäßig Sicherheits-Patches für die eigenen Produkte, wobei im Juli außer der Reihe ein Notfall-Sicherheits-Update für Photoshop, Prelude und Bridge herausgegeben wurde. Eine Woche nach dem regulären monatlichen Sicherheits-Update veröffentlichte Adobe Sicherheitshinweise mit insgesamt 13 Schwachstellen, von denen 12 als schwerwiegend gelten. Ihre Ausnutzung kann die Ausführung von beliebigem Code ermöglichen.

Im August veröffentlichte Adobe Patches für 26 Schwachstellen in Adobe Acrobat und Adobe Reader, von denen 11 Fehler als kritisch eingestuft wurden. Die Fehler konnten ausgenutzt werden, um Sicherheitskontrollen zu umgehen, wobei 9 der kritischen Fehler die Remote-Ausführung von beliebigem Code ermöglichen.

Doch nicht nur Software für Windows ist angreifbar. Cyberkriminelle greifen zunehmend die Schwachstellen nicht gepatchter VPNs an. Eine Schwachstelle, die eine Ausführung von beliebigem Code in Citrix VPN-Appliances erlaubt und als CVE-2019-19781 bekannt ist, wurde in aktiven Exploits entdeckt. In Pulse Secure VPN-Servern wurde die Schwachstelle CVE-2019-11510 entdeckt, die das Auslesen beliebiger Dateien ermöglicht und weiterhin ein attraktives Ziel für böswillige Akteure darstellt.

Weltweit am häufigsten ausgenutzte Applikationen



Teil 4

Ausblick auf 2021

Empfehlungen von Acronis für zuverlässige Sicherheit in der aktuellen und zukünftigen Bedrohungslage

Angriffe auf Mitarbeiter im Home Office werden sich weiter verstärken

Angesichts rasant steigender COVID-19-Infektionszahlen ist nur schwer vorstellbar, dass die Pandemie in diesem Jahr ein Ende findet. Wahrscheinlicher ist jedoch, dass es sogar bis 2022 dauern könnte, bis Impfstoffe weltweit verfügbar sind. Das bedeutet, dass schlecht geschützte Mitarbeiter im Home Office auch weiterhin attraktive Ziele darstellen werden. Im Jahr 2020 haben Cyberkriminelle erkannt, dass Phishing immer noch gut funktioniert und dass Angestellte das Einfallstor zu den Unternehmensdaten sind. Wir rechnen damit, dass Angriffe auf Mitarbeiter im Home Office zunehmen und immer raffinierter werden, da mehr Cyberkriminelle an Unternehmensdaten und -systeme gelangen möchten, die sich in leeren Büros und Datenzentren befinden.

Datenexfiltration erhält größere Bedeutung als Datenverschlüsselung.

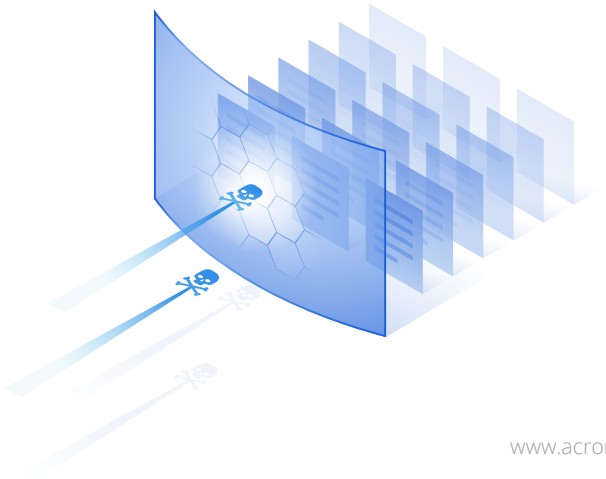
Aktuelle Ransomware-Vorfälle zeigen, dass Cyberkriminelle von jedem Angriff zu profitieren versuchen. Mehr noch: Sie stellten fest, dass Erpressungen mit gestohlenen vertraulichen Daten sehr gut funktionieren – und vielleicht sogar besser, als wenn sie die gleichen Daten einfach verschlüsseln. Aus diesem Grund rechnen wir damit, dass Datenexfiltration das Hauptziel aller Ransomware-Angriffe wird. Lösungen für Data Protection sowie zur Verhinderung von Datenverlust und Datenlecks werden im neuen Jahr sehr wichtig sein, da selbst bei einer geringeren Zahl neuer Ransomware-Familien die aktiven Varianten erhebliche Schäden anrichten und sehr erfolgreich sein werden. Das bedeutet, dass wir im neuen Jahr Ransomware als größte Bedrohung für Unternehmen betrachten.

Mehr Angriffe auf MSPs und kleine Unternehmen

Da mehr kleine und mittelgroße Unternehmen auf Cloud-MS(S)Ps setzen, nutzen mehr Cyberkriminelle dies als Angriffsvektor. In den Jahren 2019 und 2020 erkannten die böswilligen Akteure, dass Angriffe auf MSPs sehr effizient und gerade kleinere Anbieter schlecht geschützt sind. Eine Attacke auf einen MSP trifft Dutzende Unternehmen, die bei diesem MSP Kunde sind. Damit können die Angreifer mehr Geld durch Ransomware-Infektionen oder Banking-Trojaner erbeuten. Außerdem lassen sich gut etablierte Tools wie Remote-Zugriffs- und Software-Bereitstellungs-Tools missbrauchen. Solche Angriffe werden wahrscheinlich weltweit zunehmen, da sowohl kleine Unternehmen als auch MSPs einerseits nicht für ernsthafte Attacken gerüstet sind, andererseits mittelgroße Lösegelder zahlen können.

Cloud im Visier

Während des Lockdowns haben viele Unternehmen ihre Services in die Cloud gestellt. Häufig wurde die Konfiguration jedoch hastig durchgeführt und ist daher nicht zuverlässig abgesichert, was Cloud-Applikationen und Daten-Services im Internet offenlegt. Dieses Szenario bietet Angreifern die Möglichkeit, auf Daten zuzugreifen und sie zu exfiltrieren, wie wir bereits bei Datenschutzverletzungen in S3 Data Buckets sowie Elastic Search-Datenbanken beobachten konnten. Desweiteren hat das Identitäts- und Zugriffsmanagement häufig noch immer nicht den Stellenwert, den es verdient – obwohl Identität mittlerweile die neue Peripherie darstellt. Aus diesem Grund gehen wir davon aus, dass die Überwachung des Benutzerverhaltens sowie dynamische Zugriffskontrollen verstärkt eingeführt werden.



Ransomware sucht sich neue Ziele

Ransomware-Angriffe richten sich nicht mehr nur gegen Windows- und Mac-Computer. Die Angreifer versuchen, Zugriff auf Cloud-Umgebungen zu erlangen, da Cloud-Datenbanken und Container lukrative Ziele darstellen. Innerhalb von Unternehmen sind die unzureichend geschützten Prozesssteuerungssysteme auf der OT-Seite ein weiteres interessantes Erpressungsziel. Für Privatanwender kann die Zunahme von IoT-Geräten (Internet of Things) insbesondere in Verbindung mit 5G zu neuen Infektionsherden führen. Dabei müssen die Angriffe noch nicht einmal sonderlich raffiniert sein – es genügt schon, DDoS-Attacken (Distributed Denial of Service) zu generieren, um die Opfer zur Zahlung von Lösegeld zu motivieren.

Angreifer setzen verstärkt auf Automatisierung – die Zahl der Malware-Varianten steigt

Cyberkriminelle setzen alles daran, ihre Prozesse so weit wie möglich zu automatisieren. Mithilfe von Big Data-Analyse-Tools und Machine Learning können sie schneller neue Opfer finden und personalisierte Spam-Nachrichten generieren. Daher dienen die Crimeware-as-a-Service- sowie Partnerprogramme als zusätzlicher Beschleuniger. Nach der ersten Zugriffs- und Ausführungsphase nutzen die meisten Gruppen jedoch noch immer manuelle Methoden, um ihre Malware im Unternehmensnetzwerk zu verbreiten. Unabhängig davon werden wir eine Zunahme bei bereits bekannten Angriffsmethoden erleben, die unterschiedlich stark personalisiert sind.

Empfehlungen von Acronis für zuverlässige Sicherheit in der aktuellen und zukünftigen Bedrohungslage

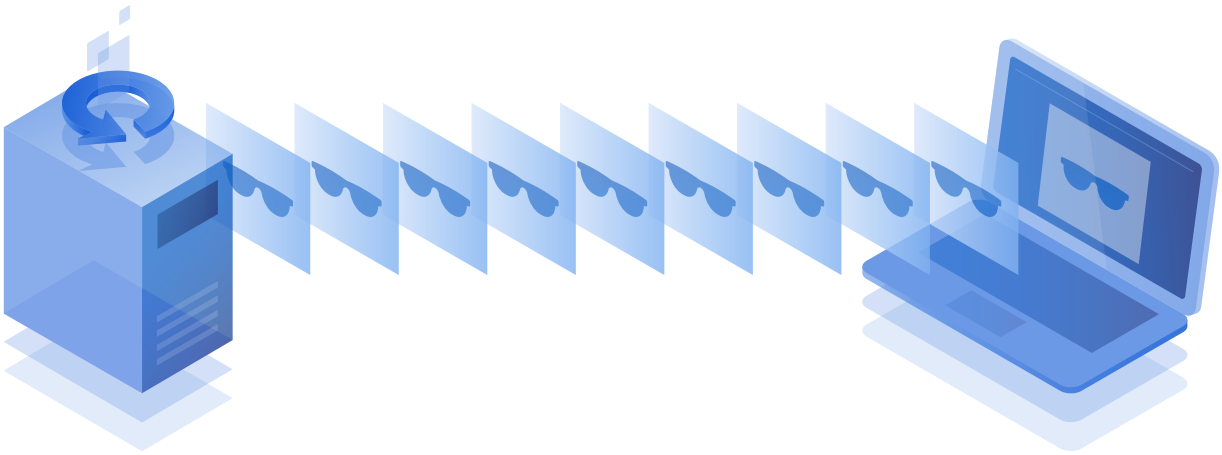
Aktuelle Cyberangriffe, Datenlecks und Ransomware-Ausbrüche weisen auf einen wunden Punkt hin: Die Cyber Security kann nicht mehr Schritt halten. Ein Grund für diesen Rückstand sind unzureichende Technologien sowie menschliche Fehler, die durch cleveres Social Engineering ausgelöst werden. In Fällen, in denen eine Backup-Lösung gut funktionierte und nicht kompromittiert wurde, dauert es meist Stunden und Tagen, um Systeme (mitsamt ihrer Daten) in einen betriebsfähigen Zustand wiederherzustellen. Backups sind unverzichtbar, wenn Cyber Security-Lösungen versagen. Gleichzeitig können Backup-Lösungen kompromittiert bzw. deaktiviert werden oder langsam arbeiten, sodass Unternehmen aufgrund von Ausfallzeiten viel Geld verlieren.

Um diese Probleme zu lösen, empfehlen wir eine integrierte Cyber Protection-Lösung wie Acronis Cyber Protect. Diese kombiniert Malware-Schutz, Schwachstellenbewertungen, Patch-Verwaltung, RMM sowie Backup-Funktionen in einem einzigen Agenten, der unter verschiedensten Windows-Betriebssystemen läuft. Dank dieser Integration können Sie die optimale Leistung gewährleisten, Kompatibilitätsprobleme beseitigen und eine schnelle Wiederherstellung sicherstellen. Wenn eine Bedrohung übersehen wurde oder erst erkannt wird, während sie Ihre Daten verändert, wird der Agent die unveränderten Daten sofort aus dem Backup wiederherstellen.

Ein solches automatisiertes Recovery ist mit einem Anti-Malware-Agenten nicht möglich. Ihre Malware-Schutzlösung kann vielleicht die Bedrohung stoppen, doch einige Daten sind wahrscheinlich bereits verloren. Ein Backup-Agent weiß nicht automatisch davon und die Daten werden – wenn überhaupt – nur langsam wiederhergestellt.

Natürlich versucht Acronis Cyber Protect Cloud, Datenwiederherstellungen unnötig zu machen, indem die Lösung Bedrohungen erkennt und beseitigt, bevor diese Ihre Umgebung beeinträchtigen können. Möglich wird dies durch unsere erweiterten und mehrschichtigen Cyber Security-Funktionen.

Dennoch sollten Unternehmen und Privatanwender selbst dann nicht grundlegende Sicherheitsregeln vergessen, wenn sie moderne Lösungen wie Acronis Cyber Protect nutzen.



Patches für Ihr Betriebssystem und Ihre Applikationen

Die Installation von Patches ist unverzichtbar, da viele erfolgreiche Angriffe ungepatchte Schwachstellen ausnutzen. Mit einer Lösung wie Acronis Cyber Protect profitieren Sie von integrierten Schwachstellenbewertungen und Patch-Verwaltungsfunktionen. Wir verfolgen alle entdeckten Schwachstellen und veröffentlichten Patches, damit Administratoren und Techniker problemlos alle Endpunkte mit einer flexiblen Konfiguration und detaillierten Berichten patchen können. Acronis Cyber Protect unterstützt nicht nur alle integrierten Windows-Anwendungen, sondern auch mehr als 100 beliebte Drittanbieter-Applikationen wie Telekommunikations-Tools (z. B. Zoom und Slack) und VPN-Clients, die bei der Arbeit im Home Office zum Einsatz kommen. Achten Sie darauf, schwerwiegende Schwachstellen zuerst zu patchen und den Erfolgsbericht zu kontrollieren, um sicherzustellen, dass die Patches ordnungsgemäß installiert wurden.

Wenn Sie nicht über Acronis Cyber Protect verfügen bzw. keine Software zur Patch-Verwaltung verwenden, ist das deutlich schwieriger. Zumindest müssen Sie gewährleisten, dass Windows alle benötigten Updates erhält und diese schnellstmöglich installiert werden. Sehr häufig ignorieren Benutzer Systemmeldungen, in denen Windows einen Neustart anfordert – was ein großer Fehler ist. Prüfen Sie, ob automatische Updates für Produkte gängiger Software-Anbieter wie Adobe aktiviert sind und Anwendungen wie Acrobat Reader immer umgehend aktualisiert werden.

Vorsicht vor Phishing-Versuchen und verdächtigen Links

Das Thema COVID-19 wird heute weithin in Phishing-Versuchen verwendet. Es ist jedoch damit zu rechnen, dass die Zahl dieser böswilligen Aktivitäten noch weiter steigen wird, weshalb alle Angestellten im Home Office darauf vorbereitet sein sollten. Themenbezogenes Phishing sowie böswillige Websites tauchen jeden Tag in großer Zahl auf und werden normalerweise auf Browser-Ebene gefiltert. Mit einer Cyber Protection-Lösung wie Acronis Cyber Protect profitieren Sie jedoch von dedizierten URL-Filterungsfunktionen. Die gleichen Funktionen sind auch für Endpunkt-Schutzlösungen verfügbar, obwohl Acronis Cyber Protect eine spezielle Kategorie für gesundheitsbezogene Themen besitzt, die mit größerer Priorität aktualisiert wird. Böswillige Links können aus beliebigen Quellen wie E-Mail, Forenbeiträgen sowie Instant Messaging-Applikationen stammen. Klicken Sie nicht auf Links, die für Sie keinen Nutzen haben und die Sie nicht erwarten.

Phishing oder böswillige Anhänge können ebenso wie böswillige Links per E-Mail eingehen. Bei Anhängen müssen Sie stets deren Quelle überprüfen und sicherstellen, dass Sie die Anhänge erwarten. Jeder Anhang sollte mit Ihrer Malware-Schutzlösung gescannt werden.

VPN bei der Arbeit mit Geschäftsdaten

Ganz gleich, ob Sie aus der Ferne auf Unternehmensquellen und Services zugreifen oder lediglich Webressourcen aufrufen und Kommunikations-Tools nutzen, sollten Sie stets ein VPN verwenden. Ein VPN verschlüsselt Ihren gesamten Datenverkehr, sodass Hacker mit Ihren übertragenen Daten nichts anfangen können. Wenn Ihr Unternehmen über eine VPN-Richtlinie verfügt, erhalten Sie sehr wahrscheinlich entsprechende Anweisungen von Ihrem Administrator oder MSP-Techniker. Wenn Sie Ihren Arbeitsplatz selbst absichern müssen, sollten Sie bekannte und empfohlene VPN-Applikationen und -Services nutzen, die auf Software-Marketplaces oder direkt von Anbietern erhältlich sind.

Ordnungsgemäße Funktion Ihrer Cyber Security-Lösung

In Acronis Cyber Protect sind gut ausbalancierte und optimierte Sicherheitstechnologien integriert. So besitzt das Acronis Produkt mehrere Erkennungs-Engines, die einer integrierten Windows-Lösung vorzuziehen sind.

Es genügt jedoch nicht, dass der Malware-Schutz installiert ist: Er muss auch ordnungsgemäß konfiguriert sein. Das bedeutet:

- **Mindestens einmal täglich sollte ein vollständiger Scan durchgeführt werden.**
- **Das Produkt benötigt täglich oder stündlich Updates (je nachdem, wie oft sie zur Verfügung gestellt werden).**
- **Das Produkt sollte mit Erkennungs-mechanismen in der Cloud verbunden sein, was im Fall von Acronis Cyber Protect die Acronis Cloud Brain Komponente ist. Sie ist standardmäßig aktiv, Sie müssen jedoch sicherstellen, dass das Internet verfügbar und nicht versehentlich vom Malware-Schutz blockiert ist.**
- **On-Demand- und On-Access-Scans (in Echtzeit) sollten aktiviert sein und auf jede neu installierte oder ausgeführte Software reagieren.**

Wichtig: Ignorieren Sie niemals Meldungen Ihres Malware-Schutzes. Lesen Sie diese sorgfältig durch und achten Sie darauf, dass die Lizenz gültig ist (sofern Sie die Bezahlversion eines Sicherheitsanbieters nutzen).

Halten Sie Kennwörter und Arbeitsplatz unter Verschluss

Unser letzter Sicherheitstipp: Achten Sie darauf, dass Ihre eigenen Kennwörter und die Ihrer Mitarbeiter stark und vertraulich sind. Geben Sie die Kennwörter niemals weiter. Nutzen Sie für jeden Service ein eigenes und langes Kennwort und verwalten Sie diese Kennwörter mit einer Kennwort-Manager-Software. Die Alternative sind lange Passphrasen, die sich leicht merken lassen. Kennwörter mit acht Zeichen lassen sich heute mit Brute-Force-Angriffen leicht knacken.

In einem sicheren Produkt wie Acronis Cyber Cloud oder Acronis Cyber Backup speichern wir nirgends Kennwörter, sodass kein unzulässiger Zugriff auf Daten möglich ist.

Abschließend sollten Sie nie vergessen, Ihren Laptop oder Desktop zu sperren und den Zugriff darauf zu beschränken – selbst dann, wenn Sie im Home Office arbeiten. Es gibt zu viele Fälle, in denen vertrauliche Informationen von einem nicht gesperrten PC gestohlen werden wurden – selbst aus einiger Entfernung.

Weitere Ressourcen

On-Demand-Webinar: Cybersecurity 2021 – The Expected Threat Landscape

Whitepaper: Acronis Cyber Readiness Report

Kostenloses Tool: Fragebogen für die Cybersicherheitsanalyse

Acronis

Über Acronis

Acronis vereint Data Protection und Cyber Security in einer integrierten, automatisierten Cyber Protection-Lösung, die mit Verlässlichkeit, Verfügbarkeit, Vertraulichkeit, Authentizität und Sicherheit (kurz: SAPAS) die Herausforderungen der modernen digitalen Welt bewältigt. Dank flexibler Deployment-Modelle, die die Anforderungen von Service Providern und IT-Verantwortlichen erfüllen, bietet Acronis hervorragende Cyber Protection für Daten, Applikationen und Systeme mit innovativen Lösungen, die Virenschutz der nächsten Generation, Backup, Disaster Recovery und Verwaltung für den Endpunktschutz umfassen. Unterstützt durch preisgekrönten KI-basierten Malware-Schutz und Blockchain-basierte Authentifizierung schützt Acronis Ihre Daten in allen lokalen, Cloud-basierten und hybriden Umgebungen – zu geringen und vorhersagbaren Kosten.

Acronis wurde 2003 in Singapur gegründet und ist seit 2008 in der Schweiz eingetragen. Heute beschäftigt das Unternehmen mehr als 1.500 Mitarbeiter an 33 Standorten in 18 Ländern. Den Acronis Lösungen vertrauen bereits mehr als 5,5 Millionen Privatanwender und 500.000 Unternehmen – einschließlich 100 % der Fortune 1000-Unternehmen und erstklassige Profisport-Teams. Acronis Produkte können über mehr als 50.000 Partner und Service Provider in über 150 Ländern und in mehr als 40 Sprachen erworben werden. Weitere Informationen finden Sie unter www.acronis.com.