Vorhersagen für 2021: Ein Jahr voller Chancen und Herausforderungen

Check Point sieht verschiedene Gefahren im Jahr 2021 auf die digitale Welt zukommen. Dazu gehören zusätzliche Angriffe mit Covid-19-Bezug, die Weiterentwicklung von bewährter Malware, neue Angriffsarten gegen den 5G-Mobilfunkstandard wie auch das Internet of Things, Ausweitung virtueller Kriege sowie Schwierigkeiten bei Datenschutz und Privatspähre.

San Carlos, Kalifornien – 10. November 2020 – Check Point® Software Technologies Ltd. (NASDAQ: CHKP), ein weltweit führender Anbieter von Cyber-Sicherheitslösunge, veröffentlicht die eigenen Vorhersagen zur IT-Sicherheit für das Jahr 2021 und benennt die zentralen Bedrohungen für Unternehmen.

Check Point stellt fest, dass die Auswirkungen der Änderungen, die wegen der Covid-19-Pandemie eingeführt wurden, weiterhin im Mittelpunkt der IT- und Sicherheitstabteilungen von Organisationen weltweit stehen werden. 81 Prozent der Unternehmen haben ihre Belegschaft massenhaft auf Remote Working umgestellt und 74 Prozent planen, die Fernarbeit dauerhaft zu ermöglichen. Check Point warnt außerdem vor neuartigen Bedrohungen durch Ransomware und Bot-Netze sowie vor den Herausforderungen bei der Sicherung der aufkommenden 5G-Netzwerke und der Zunahme damit verbundener Geräte, also des Internet of Things (IoT).

„Die Covid-19-Pandemie führte dazu, dass praktisch jede Organisation aus dem Gleichgewicht geriet und gezwungen war, ihre bestehenden Geschäfts- und Strategiepläne beiseite zu legen, um sich schnell auf die Bereitstellung sicherer Remote Connectivity in großem Maßstab für ihre Belegschaft zu konzentrieren. Die Sicherheits-Teams mussten sich auch mit Bedrohungen gegen ihre neuen Cloud-Umgebungen auseinandersetzen, da Hacker die Pandemie ausnutzen möchten: 71 Prozent der Sicherheitsexperten berichteten daher von einer allgemeinen Zunahme von Cyber-Bedrohungen seit Beginn der Lockdowns“, berichtet Sonja Meindl, Country Manager Östrreich und Schweiz bei Check Point Software Technologies, und erklärt weiter: „Eines der wenigen vorhersehbaren Dinge im Bereich der Cyber-Sicherheit ist, dass die Akteure stets versuchen werden, größere Ereignisse oder Einschnitte – wie Covid-19 oder die Einführung von 5G – zu ihrem Vorteil zu nutzen. Um Bedrohungen einen Schritt voraus zu sein, müssen Organisationen handeln und keinen Teil ihrer Angriffsfläche ungeschützt oder unüberwacht lassen. Andernfalls laufen sie Gefahr, das nächste Opfer ausgeklügelter, sogar gezielter Angriffe zu werden.“

Check Points Vorhersagen lassen sich in drei Kategorien zusammenfassen: Entwicklungen rund um Covid-19, Konflikte in den Bereichen Malware, Privatspähre und virtueller Krieg (cyber-war), Ausbau von 5G und des IoT.

Entwicklung mit Bezug zur Corona-Krise

- **Absicherung des ‚Next Normal‘:** Im Jahr 2021 wird Covid-19 weiterhin Auswirkungen auf das Leben, die Geschäfte und allgemein die Gesellschaft haben; diese Auswirkungen aber werden sich im Laufe des Jahres ändern. Die Welt muss daher auf eine Reihe von ‚Neuen Normalzuständen‘ vorbereitet sein, wenn sie auf diese Veränderungen reagieren möchte. Am Anfang stand in diesem Jahr die schnelle Umstellung vieler Mitarbeiter auf die Arbeit im Home Office. Nun müssen Organisationen ihre so neu entstandenen Fernzugriffsnetzwerke und Cloud-Umgebungen ordentlich absichern, um ihre Anwendungen und Daten zu schützen. Dies bedeutet, dass die Durchsetzung und

Automatisierung der Richtlinien und Sicherheitslösungen an allen Punkten und auf allen Geräten des Netzwerks – von den Handys und sonstigen Endgeräten der Mitarbeiter über das IoT bis hin zu Clouds – erfolgen muss. Fortschrittliche Angriffe lassen sich nur auf diese Weise stoppen, sonst breiten sie sich schnell in Unternehmen aus. Die Automatisierung der IT-Sicherheit ist von entscheidender Bedeutung, da 78 Prozent der Unternehmen angeben, dass es ihnen an Fachwissen, weil Fachkräften, mangelt.

- **Keine Heilung für Covid-19-bedingte Schwachstellen:** Da Covid-19 die Schlagzeilen weiter beherrschen wird, werden Nachrichten über Impfstoffe oder neue nationale Restriktionen weiterhin in Phishing-Kampagnen verwendet werden. Besonders Pharmakonzerne, als Entwickler der Impfstoffe, werden das Ziel virtueller Angriffe von Kriminellen oder Nationalstaaten sein.
- **Virtueller Unterricht als Zielscheibe:** Schulen und Universitäten mussten sich auf die groß angelegte Nutzung von E-Learning-Plattformen umstellen, weswegen es nicht überrascht, dass der Sektor im August, vor Beginn des Semesters, einen Anstieg der wöchentlichen Cyber-Angriffe um 30 Prozent verzeichnete. Diese Attacken werden auch im kommenden Jahr die Schüler und Studenten zu stören versuchen.

Malware, Privatsphäre und virtueller Krieg

- **Die Ransomware-Masche der ‚Doppelten Erpressung' (Double Extortion):** Im 3. Quartal 2020 gab es einen starken Anstieg von Ransomware-Attacken kombiniert mit, Double Extortion': Hacker extrahieren zunächst große Mengen sensibler Daten, bevor sie die Datenbanken eines Opfers verschlüsseln. Dann drohen sie damit, diese Daten zu veröffentlichen, wenn kein Lösegeld gezahlt wird, was zusätzlichen Druck auf die Organisationen ausübt, den Forderungen der Hacker nachzukommen.
- **Bot-Netz-Armeen auf dem Vormarsch:** Hacker haben viele Malware-Familien zu Bot-Netzen entwickelt, um Heerscharen von infizierten Computern aufzubauen, über die sie Angriffe starten. Emotet, die im Jahr 2020 am häufigsten verwendete Malware, begann als Banking-Trojaner, hat sich aber zu einem der hartnäckigsten und vielseitigsten Bot-Netze entwickelt. Es ist in der Lage, eine Reihe von schädlichen Exploits zu starten, von Lösegeldzahlungen bis hin zu Datendiebstahl, weil es andere Schadprogramme als Türöffner herunterlädt.
- **Nation gegen Nation:** Cyber-Angriffe durch staatliche Akteure werden weiterhin zunehmen, sei es zur Spionage oder zur Beeinflussung von Ereignissen in anderen Ländern. Microsoft berichtete, dass 89 Prozent der nationalstaatlichen Hacker-Angriffe im vergangenen Jahr von Akteuren aus nur drei Ländern gestartet wurden. In den letzten Jahren lag der Schwerpunkt der Verteidiger auf der Sicherung nationaler kritischer Infrastrukturen (KRITIS), und dies ist zwar nach wie sehr wichtig, doch bedeutsam wird es, die Auswirkungen von Angriffen gegen andere staatliche Sektoren einzudämmen. Dazu zählen das Gesundheitswesen, die Bildung und Behörden. Ein Fallbeispiel ist die gegen die Mongolei gerichtete Kampagne namens Vicious Panda (bösartiger Panda) vom März 2020.
- **Deepfakes als Waffe:** Die Techniken zu Erschaffung gefälschter Videos oder Tonaufnahmen sind so weit fortgeschritten, dass sie zur Schaffung gezielt manipulierender Inhalte geworden sind. Der allgemeine Name dafür lautet ‚Deepfake'. So lassen sich Meinungen, Aktienkurse oder Völker beeinflussen. Anfang 2020 veröffentlichte eine politische Gruppe in Belgien ein gefälschtes Video, worin die belgische Premierministerin Sophie Wilmès eine Rede hält, in der sie Covid-19 mit Umweltschäden in Verbindung bringt und zu Maßnahmen gegen den Klimawandel aufruft. Viele Zuschauer glaubten, die Rede sei echt. Mit weniger Aufwand könnten solche Techniken für Voice-

Phishing missbraucht werden, um die Stimme eines Vorstandes nachzuahmen und Authentifzierungen mittels Stimme zu umgehen oder Hochstapelei am Telefon zu begehen.

- **Illusion der Privatspähre:** Den meisten Menschen ist nicht bewusst, wie groß die Zahl der oft sehr intimen personenbezogenen Informationen ist, die ihre Mobil-Geräte bereits verschiedenen Leuten preis geben. Apps, die einen breiten Zugang zu den Kontakten, Nachrichten und E-Mails der Menschen fordern, oder im Hintergrund den Standort und die Fingerbewegungen auslesen sind nur ein Teil des Problems. Dieses wurde wegen fehlerhaften Covid-19-Anwendungen zur Kontaktverfolgung – die sogenannten Corona-Apps – verstärkt, weil sehr viele unsauber auf den Markt kamen und die Privatspähre der Nutzer nicht ausreichend schützten, sodass Daten über Einzelpersonen durchsickerten. Und das bei legalen Applikationen: Malware gegen Mobiltelefone, die Bankdaten von Nutzern stiehlt, falsche Apps, die sich als echte Apps tarnen, oder solche, die kostenpflichtigen Klickbetrug bei Werbeanzeigen begehen, sind eine große und wachsende Bedrohung.

Neue Plattformen für 5G und IoT

- **Vorteile und Herausforderungen des 5G-Mobilfunkstandards:** Die total vernetzte Gesellschaft und Hochgeschwindigkeitswelt, die 5G verspricht, bietet Kriminellen und Hackern neue und sehr gefährliche Möglichkeiten. Sie können Angriffe starten und Störungen verursachen, indem sie auf diese hohe Konnektivität abzielen. Sogenannte eHealth-Geräte im Bereich der Medizin werden Daten über das Wohlbefinden der Nutzer sammeln, vernetzte Autodienste werden die Fahrten der Nutzer überwachen, und intelligente Anwendungen für Städte werden über Smartphones die Bewegungen der Bürger auslesen und Informationen darüber sammeln, wie diese Nutzer ihr Leben gestalten. Diese gewaltige Datenmenge von ständig eingeschalteten 5G-Geräten muss Verletzungen, Diebstahl und Manipulation geschützt werden, um die Privatsphäre und die IT-Sicherheit zu gewährleisten – zumal viele dieser Daten die Unternehmensnetzwerke und deren Sicherheitskontrollen umgehen werden.
- **Internet der Bedrohungen:** Mit der Einführung von 5G-Netzwerken wird sich die Zahl der angeschlossenen IoT-Geräte massiv ausweiten – und damit die Anfälligkeit der Netzwerke für groß angelegte Multi-Vektor-Cyber-Angriffe massiv steigen. IoT-Geräte und ihre Verbindungen zu Netzwerken und Cloud-Umgebungen sind weiterhin ein schwaches Glied in der Sicherheitskette: Es ist schwierig, einen vollständigen Überblick aller Geräte zu erhalten, und sie stellen komplexe Sicherheitsanforderungen. Die Welt braucht einen umfassenden Ansatz für die künftige IoT-Sicherheit, bestehend aus bewährten und neuen Kontrollen, um diese ständig wachsenden Netzwerke in allen Branchen und Geschäftsbereichen angemessen zu schützen.

Alle Berichte von Check Point finden Sie unter: https://blog.checkpoint.com/
Alle Berichte des Check Point Research Teams finden Sie unter: https://research.checkpoint.com/

Folgen Sie Check Point auf:
Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Folgen Sie Check Point Research hier:
Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_

Über Check Point Research
Check Point Research bietet führende Cyber-Bedrohungsinformationen für Check Point Software-Kunden und die größere Intelligenz-Community. Das Forschungsteam sammelt und analysiert globale Cyber-Angriffsdaten, die auf der ThreatCloud gespeichert sind, um Hacker fernzuhalten und gleichzeitig sicherzustellen, dass alle Check Point Produkte mit den neuesten Schutzmaßnahmen aktualisiert werden. Das Forschungsteam besteht aus über 100 Analysten und Forschern, die mit anderen Sicherheitsanbietern, der Strafverfolgung und verschiedenen CERTs zusammenarbeiten.

Über Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) ist ein führender Anbieter von Cyber-Sicherheitslösungen für Unternehmen und Regierungen weltweit. Die Lösungen schützen Kunden vor Cyber-Angriffen der 5. Generation mit einer branchenführenden Fangrate von Malware, Ransomware und anderen gezielten Angriffen. Check Point bietet die mehrstufige Sicherheitsarchitektur ‚Infinity' Total Protection mit Gen V Advanced Threat Prevention, die alle Netzwerke, Clouds und mobilen Operationen eines Unternehmens, sowie die Geschäftsinformationen auf diesen Geräten, vor allen bekannten Angriffen schützt. Check Point liefert zudem das umfassendsten und intuitivsten Single Point of Control Management-System der Branche. Check Point schützt über 100 000 Unternehmen jeder Größe in der ganzen Welt.
Check Point Alps (Schweiz und Österreich) mit Sitz in Zürich und Wien beschäftigt rund 50 Mitarbeitende.

Pressekontakt:
Check Point Software Technologies (Switzerland) AG
Sonja Meindl
Tel: +41 44 316 64 44
E-Mail: smeindl@checkpoint.com

Jenni Kommunikation
Sylvana Zimmermann
Tel: +41 44 388 60 80
E-Mail: sylvana.zimmermann@jeko.com

