IT-Security-Trends

„Cyberangriffe werden professioneller und destruktiver“

Was sind die wichtigsten Trends der IT-Sicherheit? Wie können Unternehmen mit der sich verändernden Bedrohungslandschaft Schritt halten? Und was bedeutet all das für den Channel? Über diese Fragen sprachen wir mit Carsten Dietrich, Program Director der IBM X-Force Threat Intelligence und Siegfried Markiefka, Senior Business Development Manager bei Tech Data Advanced Solutions.

Schlagzeilen machen gerade Fälle von sogenannten Ransomware-Attacken. Bei diesen werden wichtige Computerdateien verschlüsselt und erst gegen Zahlung eines Lösegelds wieder freigegeben. Wie schätzen Sie aktuell die Gefahr durch Ransomware ein?

Carsten Dietrich: Die Bedrohungslage ist hoch. Denn die eingesetzten Verschlüsselungstrojaner, auch als Ransomworms bezeichnet, werden immer aggressiver und destruktiver. Sie haben die Macht, Geschäftsprozesse von Unternehmen komplett zum Stillstand zu bringen. Erst im Dezember hat eine Ransomware-Attacke die komplette Fertigung und Montage eines deutschen Maschinenbauers lahmgelegt. Der Trend zu destruktiven Ransomworms tritt verstärkt seit 2017 auf. Verschlüsselungstrojaner wie WannaCry, NotPetya oder Bad Rabbit haben im selben Jahr einen weltweiten Schaden von über 8 Milliarden US-Dollar angerichtet.

Eine weitere Stoßrichtung vieler Cyberangriffe ist das Ausspionieren wichtiger Unternehmensinformationen. Wie sieht die Situation dort aus?

Carsten Dietrich: In unseren jährlichen X-Force Threat Intelligence Index Reports stellen wir seit Jahren eine zunehmende Professionalität der Cyperkriminellen fest. Das wirkt sich auch auf die Industriespionage aus. Gezielt versuchen die Hacker, Schwachstellen in den IT-Systemen der Unternehmen ausfindig zu machen. Ist diese gefunden, wird Schadsoftware unbemerkt platziert. Stück für Stück breitet sich die Malware im gesamten Netzwerk aus und die Cyberkriminellen erhalten einen dauerhaften Zugriff auf wichtige Daten und Informationen. Diese als ‚Advanced Persistent Threats (APT)’ bekannte Angriffsart stellt eine massive Gefährdung dar. Sie setzt ein hohes technisches Know-how auf Seiten der Angreifer voraus. Besonders fatal für die Opfer: Durchschnittlich dauert es vier Monate, bis die APT-Angriffe von den Unternehmen entdeckt werden.

Als einen weiteren Security-Trend identifiziert der IBM X-Force Sicherheitsreport 2018 die Kryptowährungskriminalität. Was ist darunter zu verstehen?

Carsten Dietrich: Bitcoin und Co. rücken immer mehr in den Fokus der Cyberkriminellen. Dabei setzen die Angreifer sogenannte ‚Coin Mining Malware’ ein. Diese Variante von Schadsoftware kapert Computer und Smart Home-Geräte und nutzt deren Rechenleistung für das illegale Krypto-Mining, also das Erzeugen von Bitcoins. Dafür genügt schon der Besuch einer präparierten Webseite, die Schwachstellen in den Web-Browsern der Internet-Anwender ausnutzt. Oder Geräte werden als Teil eines Botnetzes für das Schürfen von Bitcoins eingespannt. Oft bleiben solche Angriffe für lange Zeit unbemerkt.

Seit dem 25. Mai 2018 ist die Datenschutzgrundverordnung (DSGVO) im gesamten EU-Raum anzuwenden. Wie wirkt sich die EU-DSGVO auf die IT-Security aus?

Siegfried Markiefka: Die EU-DSGVO wird zum Dreh- und Angelpunkt für die IT-Sicherheitsstrategien von Unternehmen. Kompromittierte Datensätze sind ab sofort kein Bagatell-Vergehen mehr. In Summe wurden in den Jahren 2016 und 2017 weltweit knapp 7 Milliarden Datensätze gehackt. Das kann sich im Zeitalter der Datenschutzgrundverordnung kein Unternehmen mehr leisten. Ansonsten drohen Bußgelder, die bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes betragen können. Gefragt sind deshalb Konzepte und Maßnahmen für mehr Datenschutz und Datensicherheit. Deutsche Unternehmen haben das erkannt.

Was macht Sie da so sicher?

Siegfried Markiefka: In der aktuellen Studie „Digital Infrastructure 2020 – IT-Infrastruktur für das digitale Zeitalter' von Tech Data und Crisp Research wurden auch die zentralen Innovations- und Investitionsbereiche deutscher Unternehmen untersucht. Demnach sagen 50 Prozent der befragten IT- und Business-Entscheider, dass Investitionen in den Datenschutz und in die Erfüllung der DSGVO einen großen oder sehr großen Beitrag für die IT-Security leisten.

Wie werden sich die Security-Ausgaben deutscher Unternehmen im nächsten Jahr entwickeln?

Siegfried Markiefka: Laut der Studie wollen annähernd 46 Prozent der deutschen Unternehmen ihr Security-Budget im nächsten Geschäftsjahr um 10 bis 20 Prozent erhöhen. Ein Viertel der befragten IT- und Business-Entscheider sehen sogar 20 bis 50 Prozent mehr Ausgaben vor. Das zeigt: Security hat als Querschnittsthema für sämtliche IT-Prozesse einen festen Platz in der Investitionsplanung deutscher Unternehmen.

Welche Security-Maßnahmen raten Sie Unternehmen vor dem Hintergrund der sich verändernden Bedrohungslandschaft?

Carsten Dietrich: Wichtig ist der Dreiklang aus Prävention, Detektion und Reaktion. Zu Präventivmaßnahmen gehören zum Beispiel Anwendungen, die Mail-Server durch Blocken oder Quarantäne gefährlicher Spams schützen. Mit Penetrationstests können Schwachstellen in der Abwehr identifiziert werden. ‚Threat Intelligence'-Daten helfen bei der Analyse der aktuellen Bedrohungslage. Detektionsmaßnahmen werten zum Beispiel bei einem Security-Vorfall die Logdaten aus. Dadurch ist es möglich, die Größe der Cyberattacke festzustellen und die Einfallstore zu identifizieren. Kommt es zum Ernstfall, ist eine schnelle Reaktion entscheidend. Neben dem Einsatz verschiedener Technologien müssen dabei auch organisatorische Maßnahmen berücksichtigt werden: Wer wird wann informiert, wer trifft die notwendigen Entscheidungen und wer setzt die definierten technischen Maßnahmen schnellstmöglich um.

Siegfried Markiefka: Der Basisschutz und die Standard-Security-Anwendungen sind in Unternehmen fast immer vorhanden. Das allein reicht aber nicht aus, um die immer professioneller und aggressiver werdenden Cyberattacken abzuwehren. Anstatt an einzelnen Stellschrauben zu drehen, versprechen ganzheitliche Konzepte mehr Erfolg. Diese vereinen technische, organisatorische und personelle Maßnahmen in einer Gesamtlösung.

Das klingt alles nach einem langfristigen Prozess. Wo können Unternehmen kurzfristig etwas ändern?

Carsten Dietrich: Indem sie die fundamentalen Dinge der IT-Sicherheit beherzigen. Viele Cyberangriffe sind immer noch wegen veralteter Software-Versionen auf vielen Rechnern erfolgreich. Hier hilft ein aktives Patch Management, mit dem die Systeme immer auf dem aktuellen Stand sind. Eine zentrale Rolle im Security-Bereich nehmen die eigenen Mitarbeiter ein. Ein mangelndes Sicherheitsbewusstsein und ein Fehlverhalten aus Unwissenheit und Leichtsinn sind für einen Großteil der Cyberangriffe verantwortlich. Nicht beabsichtigte Aktivitäten wie eine falsch konfigurierte Cloud-Infrastruktur waren 2017 für 70 Prozent der illegal entwendeten Datensätze verantwortlich.

Siegfried Markiefka: Regelmäßige Schulungen und Security-Awareness-Programme sind ein guter Anfang. Doch können Firmen auch neue kreative Wege beschreiten wie etwa Live-Hacks, die Nutzung gefakter Phisihing-Mails und Incentives für besonders auf Sicherheit bedachte Mitarbeiter.

Was bedeuten die aktuellen Security-Trends für den Channel?

Siegfried Markiefka: Neue Chancen und neue Herausforderungen. Unternehmen benötigen externe Partner, um der Komplexität des Security-Themas gerecht zu werden. Gleichzeitig steigen jedoch die Anforderungen an das Know-how und die Lösungskompetenz des Channels. Für Systemhäuser und Integratoren bedeutet das, noch stärker als bisher zusammenzuarbeiten und auch Allianzen mit Beratern und anderen IT-Dienstleistern zu suchen. Der TÜV Trust IT aus Österreich zum Beispiel bietet dem Channel an, als Subunternehmer aufzutreten. Auf diese Weise kann der Partner sein Angebot um zusätzliche Beratungsexpertise erweitern, bleibt aber beim Kunden erster Ansprechpartner.

Auf welche Weise unterstützt Tech Data Advanced Solutions den Channel bei den beschriebenen Security-Herausforderungen?

Siegfried Markiefka: Tech Data Advanced Solutions hat ein Ökosystem geschaffen, das auf die Vertriebs- und Marketing-Bedürfnisse seiner Partner ausgerichtet ist. Unser Ziel ist es, unsere Partner beim Kompetenz- und Know-how-Aufbau zu unterstützen und die Zusammenarbeit untereinander zu fördern. Eine wichtige Maßnahme sind dabei die TrendUp-Veranstaltungen. Mit diesem Veranstaltungsformat wollen wir über Trends und Zukunftsthemen der IT informieren. Unsere Partner sollen Fakten, Gedanken und Ideen mitnehmen, die sie in der Praxis erfolgreich für Vertrieb und Marketing anwenden können. Zentral bei den TrendUp-Events ist zudem der Networking-Gedanke.

Herr Dietrich, Herr Markiefka, vielen Dank für das Gespräch!