Wo Profis gegen Profis kämpfen.

Anschleichen, geduldig abwarten, unerkannt zuschlagen. Die Art, wie Advanced Persistent Threats IT-Systeme attackieren, Daten abgreifen und ganze Unternehmen lahmlegen, steht für die neueste Generation hochprofessioneller Cyberangriffe. Um sich vor ihnen nachhaltig zu schützen, setzen immer mehr Unternehmen auf externe Security Operations Center. Ein Dienst, den die Telekom via Cloud als SOC as a Service zur Verfügung stellt.

TEXT —— Roger Homrich

Sie heißen Operation Pawn Storm, Office Monkeys oder Fancy Bear. Chic sind sie jedoch nicht. Eher raffiniert – und bereiten Sicherheitsexperten besondere Kopfschmerzen. Denn sie agieren wie Auftragseinbrecher, sind Cybersöldner, die im Auftrag Dritter zielgerichtet Infrastrukturen von Unternehmen attackieren. Dafür nisten sie Schadsoftware unbemerkt in Netzwerke ein. Der Schädling verbreitet sich dann klammheimlich, sammelt Daten und sendet sie an Angreifer und Auftraggeber. Durchschnittlich 208 Tage dauere es, bis ein Cyberspion auffliegt, hat das Bundesamt für Sicherheit in der Informationstechnik berechnet. Oftmals jedoch noch viel länger. „Der aktuell von uns festgestellte Rekord liegt bei fünf Jahren“, sagt Dr. Alexander Schinner, IT-Forensiker bei T-Systems, der als Spurensucher Jagd macht auf Angreifer aus dem Netz (siehe Interview S. 29).

APT28 – Advanced Persistent Threats 28 – heißt eine Hackertruppe, die seit Jahren mit gezielten Angriffen ihr Unwesen treibt. Die Fancy Bears schlagen überall dort zu, wo ihre Auftraggeber sie hinschicken – wenn sie genug Geld in die Hand nehmen. So sollen die russischen Cyberkrieger sich während des US-Wahlkampfs auf den Servern der Demokraten eingenistet haben. Und vermutlich steckt APT28 hinter dem Angriff auf den Deutschen Bundestag im Mai 2015 sowie dem Hack auf Emmanuel Macron, nur wenige Tage vor der Stichwahl im französischen Präsidentschaftswahlkampf im Mai 2017.

Vorsicht bei E-Mails von „Freunden“

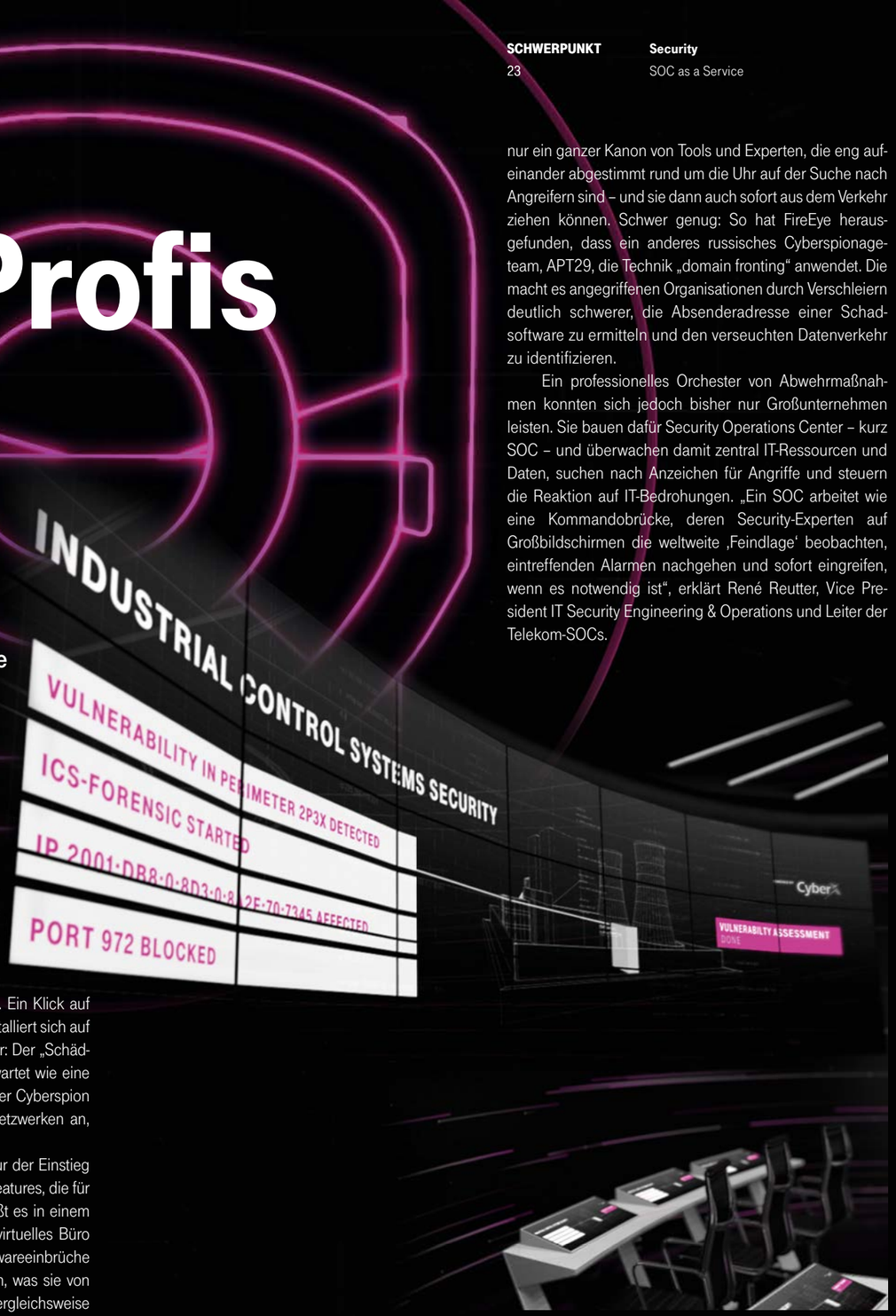
Die Vorgehensweisen der Spione sind unterschiedlich. Beliebt und simpel zugleich ist das Spearfishing. Der Hacker beobachtet sein Opfer, lernt es kennen und sendet ihm irgendwann eine unauffällige E-Mail zu. Absender: ein Bekannter, Freund oder Familienmitglied. Ein Klick auf Anhang oder Link reicht, und die Malware installiert sich auf dem Zielrechner. Es geht aber noch einfacher: Der „Schädling“ sitzt auf einer infizierten Website und wartet wie eine Zecke im Gras auf arglose Besucher. Oder der Cyberspion greift über bekannte Sicherheitslücken in Netzwerken an, die zu spät geflickt werden.

Das Installieren der Schadsoftware ist nur der Einstieg ins System. „APT28 nutzt eine Malware mit Features, die für andauernde Operationen gedacht sind“, heißt es in einem FireEye-Report. Die Hacker bauen sich ein virtuelles Büro auf, über das sie größer angelegte Softwareeinbrüche durchführen. Dafür brauchen sie Ressourcen, was sie von den Alltagshackern unterscheidet, die ihre vergleichsweise einfach gestrickten Viren und Würmer massenhaft versenden und deren Erfolge eher auf Zufall beruhen – dafür auch weniger kosten.

Zentrale Überwachung der IT-Infrastruktur

Für die Abwehr von Schädlingsmassenware reichen herkömmliche Virenscanner, Firewalls und Antiphishing-Programme in der Regel aus. Aber gegen APT hilft zumeist nur ein ganzer Kanon von Tools und Experten, die eng aufeinander abgestimmt rund um die Uhr auf der Suche nach Angreifern sind – und sie dann auch sofort aus dem Verkehr ziehen können. Schwer genug: So hat FireEye herausgefunden, dass ein anderes russisches Cyberspionageteam, APT29, die Technik „domain fronting“ anwendet. Die macht es angegriffenen Organisationen durch Verschleiern deutlich schwerer, die Absenderadresse einer Schadsoftware zu ermitteln und den verseuchten Datenverkehr zu identifizieren.

Ein professionelles Orchester von Abwehrmaßnahmen konnten sich jedoch bisher nur Großunternehmen leisten. Sie bauen dafür Security Operations Center – kurz SOC – und überwachen damit zentral IT-Ressourcen und Daten, suchen nach Anzeichen für Angriffe und steuern die Reaktion auf IT-Bedrohungen. „Ein SOC arbeitet wie eine Kommandobrücke, deren Security-Experten auf Großbildschirmen die weltweite ‚Feindlage‘ beobachten, eintreffenden Alarmen nachgehen und sofort eingreifen, wenn es notwendig ist“, erklärt René Reutter, Vice President IT Security Engineering & Operations und Leiter der Telekom-SOCs.



Fotos: T-Systems

Eng aufeinander abgestimmte Tools

Dafür steht den Abwehrteams eine ganze Reihe von Sicherheitslösungen zur Verfügung, die automatisiert die zu schützenden IT-Systeme beobachten. Diese sind über Schnittstellen mit dem SOC verbunden, sodass jeglicher Datenverkehr beobachtet und analysiert wird. Da der Aufbau und der Betrieb teuer sind und Topexperten unterschiedlicher Qualifikation gebraucht werden, setzen immer mehr Unternehmen auf extern gemanagte SOCs – und damit auf Kostenteilung.

Die Cloud macht jetzt möglich, den Schutz eines Security Operations Center auch als Dienstleistung bereitzustellen (SOC as a Service), bei dem ein Security-Provider wie die Telekom nicht länger jedes Center exklusiv für einen dedizierten Auftraggeber betreibt, sondern viele Kunden parallel aus einem SOC heraus beliefern kann.

So ermöglicht die Telekom unter anderem dem deutschen Mittelstand, Heimat der Hälfte aller Hidden Champions weltweit, Security auf einem Niveau zu beziehen, das bis vor Kurzem nur Großkonzernen zur Verfügung stand. Zugleich macht der IT-Dienstleister damit den beiden größten „Show-Stoppern“ kleinerer und mittlerer Unternehmen in Sachen Security ein Ende: Der Mittelstand muss nicht länger im War for Talents nach eigenen Experten suchen und nicht mehr selbst in eigene, teure Technik investieren. Gerade mit Blick auf den anhaltenden Fachkräftemangel, so Frank Luzsicza, Bereichsleiter ICT & Business Solutions des TÜV Rheinland, „wird Vertrauen in einen kompetenten externen Partner für Cybersecurity zu einem der wichtigsten Erfolgsfaktoren für die Absicherung des Unternehmens“.

Treiber sind Kritis und das IT-Sicherheitsgesetz

„Grundsätzlich ist das Thema SOC nicht wirklich neu“, sagt Rüdiger Peusquens, „das IT-Sicherheitsgesetz und die zunehmende Qualität der Angriffe haben allerdings erst jetzt verstärkt die Aufmerksamkeit auf das Thema gelenkt“, so der Leiter des Cyber Defense Center der Telekom, verantwortlich für den Schutz der Telekom als kritische Infrastruktur. So ist inzwischen die Kritis-Verordnung zur Umsetzung des IT-Sicherheitsgesetzes in Kraft getreten. Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Wasser, Ernährung sowie Finanzen, Transport und Verkehr müssen besondere Maßnahmen umsetzen, um die Verfügbarkeit und Sicherheit ihrer IT-Systeme sicherzustellen.

Erst im März 2017 hat ein großes Energieunternehmen das Threat- und Vulnerability-Management sowie moderne Analysemethoden zum störungsfreien Betrieb der Infrastruktur an die Telekom ausgelagert. „In einem SOC zentral sämtliche Informationen aus allen Prozesslayern eines Unternehmens zu bündeln und zu bewerten hat eine enorme Bedeutung“, so Dirk Backofen, bei der Telekom Leiter der neuen konzernweiten Business Unit Telekom Security. „Nur mit dieser Informationslage kann man die eigene Betriebsumgebung mit ihren unterschiedlichen Sicherheitsleveln

steuern.“ Dafür ist es allerdings auch nötig, auf allen Ebenen des Kundenbusiness entsprechende Security-Angebote vorzuhalten und den Kunden beraten zu können, was für seine Use-Cases die beste Kombination ist.

Dass es auch dabei viel Erfahrung braucht, um die schiere Menge möglicher Technologien richtig zu nutzen, ist nur einer der Gründe dafür, dass der Kundenbedarf an Security-Cyber-Defense-Orchestration weltweit steigt. Eine Nachfrage, der das neue, in Bonn eingerichtete SOC der Telekom Security in Kombination mit dem Cyber Defense Center der Telekom vom Herbst dieses Jahres an Rechnung tragen wird.

Im dritten Quartal dieses Jahres, so die Planung, wird das Bonner Security Operations Center, in Kombination mit dem Cyber Defense Center des Konzerns, den Betrieb zur zentralen Überwachung der IT-Infrastrukturen der Telekom-Kunden aufnehmen.

Prävention, Detektion, Response

Das verwirrende Durcheinander von Angriffs- beziehungsweise Verteidigungstechnologien, das hier beherrscht werden will, bekommt Struktur, wenn man die Arbeit eines SOC auf drei Ebenen „zerlegt“: Prävention, Detektion, Response. In anderen Worten: Wie schütze ich ein Unternehmen im Vorfeld? Wie stelle ich fest, wann die Firewall – was völlig normal ist – Ransomeware, APTs & Co. bis zum Betrieb der Systeme freien Durchgang gewährt und automatisch Lösungen wie Intrusion Prevention oder Advanced Threat Protection aktiviert werden müssen? Und wer oder was hilft 24/7/365, wenn ein System infiziert ist und ein Helferteam quasi auf Knopfdruck nottut, um remote oder on premise kürzestmögliche Reaktionszeiten zu gewährleisten? Etwa um eine Malware zu isolieren oder einen infizierten Rechner zu deinstallieren. Und das sind noch die leichteren Aufgaben des Incident Response Retainer Service, den die Telekom Security für solche Fälle bereithält. Im Zweifelsfall mindestens so wichtig sind die Rückverfolgbarkeit von Angriffen und Antworten auf Fragen wie: Was ist überhaupt passiert? Welche Daten sind verloren gegangen? Wohin wurden sie versendet? Waren Geschäftsgeheimnisse darunter? Solcherlei hoch qualifizierte Forensikexperten, wie die Telekom Security ein gutes Dutzend beschäftigt, gibt es nur sehr wenige in Europa. Doch nur sie können ermitteln, welche Wege was in welcher Form genommen hat.

Sicherheit für industrielle Anlagen

Mit Industrienetzen und verknüpften Rechner-, Mess-, Steuer- und Regelsystemen in der Produktion können APTs in der Sicherheitsarchitektur von Unternehmen eine riesige Flanke aufreißen. „Die Anlagen sind häufig mit veralteter Technologie ausgestattet und verfügen über keine Gegenmaßnahmen gegen Cyberattacken, da sie einfach nicht für den vernetzten Betrieb konstruiert wurden“, sagt Bernd Jäger, Experte für Industrial Control Systems Security (ICS) bei der Telekom. „Normale IT-Sicherheitssysteme wie IT-Firewalls können in diesem Bereich nicht eingesetzt werden, und Know-how für Cybersicherheit in Industrienetzen ist oft nur rudimentär vorhanden.“ Die Telekom weitet daher die Partnerschaftslandschaft im Security-Umfeld mit Anbietern aus, die auf Industrieanlagen zugeschnittene Sicherheitslösungen entwickelt haben. Dabei geht es im Fokus von ICS-Security darum, vor allem die Detektion möglicher Angriffe zu beschleunigen sowie die angemessenen Entscheidungen von Unternehmensverantwortlichen durch die intelligente Dosierung automatisierter Gegen- und Schutzmaßnahmen zu unterstützen. „Auch diese Lösungen sind dann bei Bedarf Bestandteil eines gemanagten Security Operations Center“, erklärt René Reutter.

Wie wichtig SOCs sein können, zeigt der Kampf gegen Doping im Sport. Möglicherweise hätte ein SOC der Welt-Anti-Doping-Agentur (Wada) viel Ärger erspart. Die Fancy Bears statteten den Datenbanken der Wada schon mehrfach einen Besuch ab – und geben das unverhohlen zu: „Grüße an alle Bewohner der Welt“, heißt es auf der Startseite von Fancybear.net, „wir stehen ein für Fair Play und sauberen Sport. Wir werden euch sagen, wie Goldmedaillen gewonnen wurden. Wir haben die Datenbank der Wada gehackt und waren schockiert über das, was wir gesehen haben.“ Manchmal kann Hacking auch sinnvoll sein.

„Ein SOC arbeitet wie eine Kommandobrücke, deren Security-Experten die weltweite ‚Feindlage‘ beobachten und sofort eingreifen können.“

RENÉ REUTTER, Leiter Telekom Security Operations Center

reutter@t-systems.com
www.t-systems.de/telekom/security-operation-center
www.t-systems.de/loesungen/cyber-security

Fotos: T-Systems