

MEDIENINFORMATION

Bonn/Potsdam/Zollikofen, 22. Mai 2019

Telekom legt aktuelle Zahlen zur Cybersicherheit vor

- 46 Millionen Angriffe auf digitale Lockfallen im April
- Telekom veröffentlicht Statistik zu Angriffen
- Konferenz für Cybersicherheit beginnt morgen in Potsdam

Die Telekom macht auf wachsende Gefahren durch Hacker aufmerksam. Anfang April hatte der Konzern 46 Millionen tägliche Angriffe auf seine Honeypots. Dies ist ein neuer Spitzenwert. Im Schnitt gab es im letzten Monat 31 Millionen Angriffe pro Tag. Im April 2018 waren es durchschnittlich noch 12 Millionen. Der April-Wert 2017 lag noch bei 4 Millionen. Die Angriffszahlen steigen exponentiell. Dies gab der Konzern im Vorfeld der morgen beginnenden Potsdamer Sicherheitskonferenz bekannt.

Honeypots sind digitale Fallen im Internet. Vergleichbar sind sie Honigködern für Bären. Der Konzern lockt damit absichtlich Angreifer an. Die Telekom analysiert die Attacken und macht aus den Erfahrungen eigene Systeme und die von Kunden sicherer. Knapp 3`000 verschiedene Fallen hatte die Telekom im April im Internet ausgelegt. Angriffszahlen auf die Köder der Telekom-Unternehmen gelten in der Branche als Haltepunkt für Cybersicherheit. Sie zeigen wie umtriebiger Hacker im Internet sind.

Dirk Backofen, Leiter Telekom Security, sagt: «Fünfzig Milliarden Geräte werden wir nächstes Jahr im Internet sehen. Jeder und alles ist vernetzt und braucht Cyber-Security. Dies schafft niemand allein. Wir brauchen die Armee der Guten. Dafür teilen wir unser Wissen für eine Immunisierung der Gesell-

schaft gegen Cyber-Attacken. Nur im Schulterschluss zwischen Politik, Wissenschaft und der Privatwirtschaft werden wir erfolgreich die Hacker in die Schranken weisen können.»

Mehr als ein Viertel der Hacker zielt auf Kontrolle über fremde Rechner

Die Telekom veröffentlicht auch eine Statistik zu Angriffen auf Lockfallen. Danach zielten 51% der Attacken auf die Netzsicherheit. Hacker konzentrierten sich dabei auf Schnittstellen für die Fernwartung von Computern. In 26% der Fälle ging es dem Angreifer um die Kontrolle über einen fremden Rechner. Rund 7% der Attacken zielten auf Passwörter. 5% der Angriffe galten Internetseiten. Die Telekom Security beobachtet täglich drei bis acht unbekannte Angriffstaktiken. Aus den im Schnitt monatlich 250 neuen Hacker-Tricks lernt der Konzern Abwehr für sich selbst und seine Kunden.

110`000 Kunden hatten im April Sorge vor Passwort-Diebstahl

Passwort-Diebstahl beschäftigt den Kundenservice der Telekom intensiv. Rund 110`000 Kunden hatten im April diese Sorge und riefen bei der Hotline an. Immer wieder fallen Kunden auf das sogenannte Phishing herein. Ausgangspunkt solcher Angriffe sind gefälschte E-Mails. Sie sehen denen von Banken, Sparkassen, Online-Versendern oder Telekom-Firmen täuschend ähnlich. Sie zielen auf Betrug ab. Opfer geben darüber Kundenkennwort oder Zugangsdaten heraus. Diese nutzt der Angreifer für seine Zwecke aus.

Angriffe durch gekaperte Computer massiv gestiegen

Heftiger werden auch die Angriffe auf Fest- und Mobilfunknetz der Telekom. So feuerten im April Botnetze 5,3 Billionen Datenpakete auf die Telekom. Im Vorjahr waren es noch 330 Milliarden. Botnetze bestehen aus einer grossen Zahl gekapert Computer oder Smartphones. Fremdgesteuert senden diese gemeinsam Datenpakete auf ein Ziel. Verträgt das Ziel den Ansturm der Daten nicht, bricht es zusammen. An den Übergängen von ihrem Netz zum Internet hat die Telekom Sensoren installiert. Diese fanden heraus: Botnetze nutzen In-

ternetsurfer von Unternehmen aus. Sie greifen an, wo Firmen zwangsläufig Datenwege freihalten. Dort schützen keine Firewalls. Wo der Internet-Browser seine Datenpakete aus dem Netz bekommt, lauern die gekaperten Zombie-Rechner.

Hacker-Industrie und KI setzen Cyberabwehr unter Druck

Neben exponentiell steigenden Zahlen registriert die Telekom Security grundsätzliche Trends bei Cyber-Attacken. So entsteht seit Jahren eine Hacker-Industrie. Gruppen spezialisieren sich auf bestimmte Angriffstypen und bieten diese an. Ein Kunde stellt sich die Services verschiedener Gruppen dann je nach Bedarf und Ziel zusammen. Nach wie vor kommen die meisten Hacker-Gruppen aus China und Russland. Dabei steigt der Anteil von Attacken mit künstlicher Intelligenz. Angriffe sind daher heute viel schneller erfolgreich. Die Cyberabwehr setzt das unter Druck. Sie kontert immer mehr mit Gegenmassnahmen in Echtzeit.

Zentrum für Cyberabwehr in Bonn schützt Telekom und Unternehmen

Das integrierte Cyber Defense und Security Operation Center (SOC) schützt die IT der Telekom. Der Konzern hat das Zentrum 2017 in Bonn gegründet. Das SOC sichert auch mehrere DAX 30-Unternehmen und eine Vielzahl weiterer Firmen. Ähnliche Zentren hat die Telekom weltweit. Alle sind miteinander vernetzt und bilden gemeinsam mit dem SOC in Bonn einen Verbund.

240 Experten wehren in den SOC's rund um die Uhr Attacken ab. Sie analysieren, welche Absicht oder Fähigkeiten Hacker haben. Und untersuchen ihre Taktik (Threat Intelligence). IT-Forensiker kommen bei kriminellen Handeln hinzu. Sie rekonstruieren Angriffe und sichern Beweise. Mit allen gewonnenen Informationen verbessert die Telekom so die eigene Technik für Cyberabwehr. Wichtige Daten liefern dabei die weltweit installierten Honeypots. Das SOC ist eines der grössten und modernsten Abwehrzentren Europas.



T-Systems in der Schweiz

Krystina Koch

Tel.: +41 (0) 78 607 26 24

E-Mail: pressoffice@t-systems.ch

Weitere Informationen für Medienvertreter: www.telekom.com/medien und www.telekom.com/fotos

<http://twitter.com/tsystemschi>

<https://www.linkedin.com/company/t-systems-schweiz/>

Über die Deutsche Telekom

[Deutsche Telekom Konzernprofil](#)

Über T-Systems

[T-Systems Unternehmensprofil](#)

Über T-Systems Schweiz

[T-Systems Schweiz Unternehmensprofil](#)