AIRBUS

DEFENCE AND SPACE

Press Release

CIS

Airbus-Prognose für den Cybersicherheitsmarkt im Jahr 2018

Bedrohungen über Social-Media- und Drahtlos-Netzwerke im nächsten Jahr besonders akut

London, 14. Dezember 2017 – Forscher von Airbus CyberSecurity haben eine Liste der wichtigsten Technologieprognosen für 2018 erstellt. Die Übersicht basiert auf Trends, die 2017 in den Security Operations Centers (SOCs) des Unternehmens in Deutschland, Frankreich und Großbritannien ermittelt wurden.

Prognose Nr. 1: Fehlende Social-Media-Sicherheitsrichtlinien werden zum ernsthaften Risiko für Unternehmen

2017 war eine regelmäßige Nutzung der Social-Media-Plattformen für die Verbreitung gefälschter Nachrichten oder die Manipulation der öffentlichen Meinung zu beobachten. Soziale Medien lassen sich zur Manipulierung von Personen („Social Engineering“) und für das Ausspionieren von Informationen nutzen und sind damit ein Einfallstor für diverse hochentwickelte Angriffe auf Unternehmen. Kriminelle und Hacker nutzen diese Plattformen bekanntermaßen für betrügerische Antiviren- und Phishing-Kampagnen oder die Verbreitung von Malware zum Schaden ihrer Opfer.

Markus Brändle, Head of Airbus CyberSecurity erklärt: „Soziale Medien verbinden Menschen weltweit und bieten in unserer digitalen Welt eine Plattform für Diskussionen und den schnellen Austausch von Ideen. Aus Sicht der Angreifer sind soziale Medien jedoch ein leichtes Ziel geworden. Gründe dafür sind die hohe Zahl von Nutzern, die sich nicht um Cybersicherheit kümmern, und die einfache und kostengünstige Zugänglichkeit dieser Plattformen. Zum Schutz gegen Social-Media-Angriffe müssen Organisationen unternehmensweite Sicherheitsrichtlinien für soziale Medien implementieren. Dazu gehört die Entwicklung von Mitarbeiter-Schulungsprogrammen zur Nutzung von sozialen Medien sowie die Erstellung von Reaktionsplänen, die im Falle einer Sicherheitsverletzung die Aktivitäten der Rechts-, Personal-, Marketing- und IT-Abteilungen koordinieren.“

Prognose Nr. 2: Angriffe auf Drahtlos-Netzwerke werden dramatisch zunehmen

Die Zahl der Angriffe auf Drahtlos-Netzwerke wird ansteigen, da Angreifer versuchen, die im Oktober 2017 öffentlich gemachte KRACK-Sicherheitslücke (Key Reinstallation Attack) auszunutzen.

Diese Lücke ermöglicht es Angreifern, den WiFi-Datenverkehr zwischen Geräten und einem WiFi-Router abzufangen, auszulesen und schlimmstenfalls sogar schädliche Daten in Websites einzubringen. Angreifer könnten über die betroffenen Geräte möglicherweise auch vertrauliche Informationen abrufen, wie beispielsweise Kreditkartendetails, Passwörter, Chat-Nachrichten oder E-Mails.

Airbus Defence and Space
81663 - Munich
Germany

Email: media.airbusdefenceandspace@airbus.com
Web: airbusdefenceandspace.com
Follow us on twitter: twitter.com/AirbusDS

Brändle: „Es ist ein Anstieg der Angriffe auf öffentliche oder offene WiFi-Verbindungen zu erwarten. Als Reaktion darauf müssen Organisationen, die ihren Kunden solche Dienste anbieten, erhöhte Sicherheitsvorkehrungen bieten. Angriffe dieser Art sind insbesondere gefährlich für Nutzer alter Geräte, die von den Anbietern nicht mehr unterstützt werden und sie so zu einem attraktiven Ziel für Cyberkriminelle macht. Diese Bedrohungen könnten auch eine verstärkte Nutzung von Virtual Private Networks (VPN) durch sicherheitsbewusste Nutzer zur Folge haben."

Prognose Nr. 3: Verschlüsselung wird Strafverfolgungsorgane weiterhin vor Herausforderungen stellen

Bedenken hinsichtlich des Datenschutzes, die verstärkte Nutzung von Cloud-Computing, die zunehmende Zahl von Datenschutzverletzungen und die Einführung einer Datenschutzgrundverordnung (DSGVO) werden dazu beitragen, dass Unternehmen künftig die End-to-End-Verschlüsselung (E2EE) als effektivste Möglichkeit der Datensicherung nutzen. Andererseits wird E2EE die Strafverfolgungsorgane vor Herausforderungen stellen, da auch Kriminelle diese Technik für Spionage und andere subversive Zwecke nutzen werden.

Brändle weiter: „Bei der Bewertung der Kosten für eine Sicherheitslösung ist es wichtig, die finanziellen Auswirkungen eines Sicherheitsvorfalls zu berücksichtigen. Nach der Einführung der Datenschutzgrundverordnung (DSGVO) könnten Organisationen im Falle einer Datenschutzverletzung mit Strafen in Höhe von bis zu 4 Prozent ihres weltweiten Umsatzes belegt werden. Die Kosten für eine Lösung sind daher immer in Relation zu den bestehenden Risiken betrachten.

Über Airbus
Airbus ist ein weltweit führendes Unternehmen im Bereich Luft- und Raumfahrt sowie den dazugehörigen Dienstleistungen. Der Umsatz betrug € 67 Mrd. im Jahr 2016, die Anzahl der Mitarbeiter rund 134.000. Airbus bietet die umfangreichste Verkehrsflugzeugpalette mit 100 bis über 600 Sitzen sowie Produkte für den Geschäftsflugverkehr. Das Unternehmen ist europäischer Marktführer bei Tank-, Kampf-, Transport- und Missionsflugzeugen und eines der größten Raumfahrtunternehmen der Welt. Die zivilen und militärischen Hubschrauber von Airbus zeichnen sich durch hohe Effizienz aus und sind weltweit gefragt.

Über Airbus CyberSecurity
Airbus CyberSecurity, eine Geschäftseinheit von Airbus Defence and Space, bietet Unternehmen, kritischen nationalen Infrastrukturen sowie Regierungs- und Verteidigungsorganisationen zuverlässige und leistungsstarke Sicherheitsdienste und -produkte zur Erkennung, Analyse und Abwehr zunehmend anspruchsvoller Cyber-Angriffe.

https://www.cybersecurity-airbusds.com

Media contact

Ambra Canale +49 162 69 88 103 ambra.canale@airbus.com