Projekt „Honeytrain“: Hacker@work

Sophos-Whitepaper zum Projekt „Honeytrain enthüllt das Vorgehen der Hacker beim Zugriff auf kritische Infrastrukturen – Registriert wurden 2,7 Millionen Zugriffsversuche, einige davon mit Erfolg – Auch das Steuerungssystem war betroffen

Wiesbaden, 18.09.2015 – In seiner Hacker-Falle „Honeytrain“ hat Sophos in Zusammenarbeit mit der Firma Koramis untersucht, wie industrielle Steuerungssysteme durch Eindringlinge identifiziert und angegriffen werden. Insgesamt registrierte Sophos 2,7 Millionen Zugriffsversuche aus aller Welt über einen Zeitraum von sechs Wochen auf ein simuliertes industrielles Steuerungssystem.

Honeytrain – der perfekte Hacker-Bluff
Beim Projekt Honeytrain handelte sich um eine originalgetreue Simulation eines U-Bahn Steuerungssystems, das mit echten Industrie-Steuerungssystemen arbeitet und originale Hard- und Software-Komponenten aus der Automatisierungs- und Leittechnik einsetzt. Videos von Überwachungskameras echter Bahnhöfe und Zugführerkabinen sorgten für die nötige optische Täuschung. Die Simulation war so perfekt, dass Angreifer den Eindruck hatten, in ein real existierendes System einzudringen.

Ziel des Projekts war es herauszufinden, wie Angriffe auf kritische Infrastrukturen ablaufen, welche Gefahren drohen und wie verbreitet das Wissen über diese Systeme in der Hacker-Gemeinde ist. Über eine kontinuierliche Angriffsanalyse und -bewertung sollte ein umfassendes Bild über die Qualität, Quantität und Aggressivität der Angreifer entstehen. Dabei diente die Simulation lediglich als exemplarisches Vorbild. Ziel des Projekts war es nicht, mögliche Angriffe auf den realen Schienenverkehr darzustellen. Spannend war vor allem die Frage, wie weit Hacker gehen. Begnügen sie sich mit dem bloßen Eindringen in die IT-Systeme? Nehmen sie Sachschäden oder gar Menschenleben in Kauf?

Angriffe zielten auf Firewall, Zugsteuerung und Überwachungskameras
34 Prozent der versuchten Attacken zielten auf die Firewall des Systems. Als ebenfalls beliebt bei den Hackern erwies sich der Mediaserver. Er verarbeitet die Streams der Überwachungskameras und bietet diese über eine Webschnittstelle an. Ihn zu hacken war in 27 Prozent der Angriffsversuche das Ziel. Die Nachbauten von Steuerungssystemen, Protokollen und HMIs (Human-Machine-Interfaces, Benutzerschnittstellen) wurden in 23 Prozent der Fälle angegangen. Sieben Prozent der Angriffe entfielen auf das Infoportal, das die Webseite eines Verkehrsverbundes originalgetrau nachstellt.

Lästiger Unfug über den Mediaserver
Einige der erfolgreichen Zugriffe erfolgten über den Mediaserver. Hier nutzen die Angreifer eine Wörterbuchattacke. Mit dieser versuchen die Angreifer, einen unbekannten Benutzer oder ein unbekanntes Passwort anhand einer umfangreichen Wörterliste zu ermitteln. Ein konkretes Ziel gab es offenbar nicht. Der Angriff auf den Mediaserver zeigt ein eher spielerisches Vorgehen. Die Hacker verfügten offenbar über kein tieferes Know-how, sahen sich neugierig im System um und verschwanden wieder. In einem der Fälle nutzten die Angreifer die Möglichkeit, um die ursprünglichen Inhalte des Webangebots kreativ umzugestalten. Die Gäste beschränkten sich jedoch darauf, das Kamerabild eines U-Bahnhofs auszutauschen gegen ein eigenes Statement, dass die Nutzung von Webcams in der Öffentlichkeit kritisiert.

Zugriff auf die Zugsteuerung
Weit gefährlicher hätte einer der erfolgreichen Angriffe auf die Zugsteuerung (HMI, Human Machine Interface) werden können. Während der Dauer des Projekts konnten vier erfolgreiche Logins auf diesen Teil des Systems festgestellt werden. Zwei erfolgten über Wörterbuchattacken.

In einem Fall gelang es den Angreifern, ein starkes Passwort zu überwinden. Anders als die ungebetenen Gäste auf dem Mediaserver verfügte diese Gruppe über eine sehr genaue Kenntnis industrieller Leitsysteme und wusste genau, in was für ein System sie eingedrungen waren. Die Hacker lasen Sicherheitseinstellungen der industriellen Komponenten über ein zentrales Tool aus und exportierten diese. In der Folge griffen die Eindringlinge auch auf die Visualisierung zu und aktivierten die Frontbeleuchtung eines Zuges. Auch schlimmeres wäre an dieser Stelle möglich gewesen.

Die meisten Angriffe aus China und den USA
Was die Herkunft der Zugriffsversuche angeht, so konnten China und die USA als führende Länder identifiziert werden, gefolgt von Frankreich, Polen und Moldawien. Deutschsprachige Länder sind kaum vertreten: nur ein Prozent der Angriffe (insgesamt 26.512) wurden aus Deutschland unternommen. Weit unter einem Prozent blieben Österreich und die Schweiz mit jeweils 166 und 243 Angriffen.

Chester Wisniewski, Sicherheitsberater bei Sophos, mahnt Unternehmen zu mehr Sorgfalt: „Schon einfache Maßnahmen können dabei helfen, kritische Infrastrukturen sicherer zu machen. Diese reichen von einem sicheren Passwort, das in einer Vielzahl der Fälle nicht genutzt wurde, bis hin zu Überlegungen dazu, welcher Teil des Systems überhaupt eine Anbindung an das öffentliche Netzwerk benötigt. Abgesicherte Systemzonen und eine SSL-Verschlüsselung hätten den die Schwierigkeiten für die Angreifer um ein Vielfaches erhöht.**“**

Sach- und Personenschäden blieben während der Dauer des Projektes aus. Das war beim Auftakt auf der CeBIT noch anders. Damals schepperte es am zweiten Tag am Sophos-Messestand kräftig. Im Live-Versuchsaufbau ließen Hacker einen Zug entgleisen.

Das Whitepaper sowie weitere Informationen zum Honeytrain-Projekt finden Sie hier:
https://www.sophos-events.com/honeytrain

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt. Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:
Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617

Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de