Fraunhofer FKIE

IHR VERLÄSSLICHER PARTNER IM HINTERGRUND

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

Die Komplexität der Bedrohungslage im Cyberraum und damit die verbundenen Gefahren für die fortschreitende Digitalisierung nehmen stetig zu. Cyberkriminalität und Cyberspionage haben sich professionalisiert, das Spektrum reicht von Diebstahl und Missbrauch persönlicher Daten, von Wirtschaftsspionage über die Schädigung kritischer Infrastrukturen bis hin zur Störung und Manipulation der Regierungs- und Verteidigungskommunikation. Nicht nur die Quantität, sondern auch die Qualität der Bedrohung hat sich spürbar verändert. Angriffe richten sich längst gezielt gegen staatliche Strukturen wie Regierungsnetze, militärische Einrichtungen, Parteien, Organisationen oder Unternehmen. Nicht nur Bedrohungen durch internationalen Terrorismus, sondern auch die Cyberkriminalität zeigen, dass sich innere und äußere Sicherheit in diesen Bereichen längst überschneiden.

Daher nehmen die Analyse und Bekämpfung existierender Cyberrisiken eine wesentliche Rolle in der komplexen Struktur von wirksamer Cyberverteidigung und Cybersicherheitspolitik ein. Aus diesem Grund gilt es, präventive Maßnahmen zur Sicherung der IT-Systeme zu ergreifen, bestehende Netze und Geräte zu überwachen sowie Bedrohungen zu analysieren und abwehren zu können.

Das Fraunhofer FKIE ist mit seinen langjährigen Erfahrungen und Forschungsarbeiten im Bereich der Cyberabwehr bestens aufgestellt, um die IT-Sicherheit für den Staat, die Bürger und die Wirtschaft zu verbessern und zu gewährleisten. Mit der Errichtung von Frühwarnsystemen, der Analyse von Cyberkriminalität und der Entwicklung sicherer und zuverlässiger IT-Schutzsysteme für die Regierungsnetze erweist sich das FKIE als verlässlicher Partner im Hintergrund. Viele dieser Schutzmaßnahmen werden insbesondere im Rahmen der Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt und betrieben. Auch Betroffene außerhalb der Regierungsnetze konnten dank der technischen Unterstützung des FKIE durch das BSI vor aktuellen Bedrohungen gewarnt und bei der Ergreifung von Gegenmaßnahmen unterstützt werden.

Die Mission des FKIE lautet »Wir arbeiten jeden Tag daran, die Welt sicherer zu machen«. Mit Blick auf die neue Dimension der Bedrohung durch die komplexen, schwer erkennbaren Cyberangriffe steht mit dem FKIE ein verlässlicher und verantwortungsvoller Partner für den Schutz und die Verteidigung der IT-Sicherheit bereit.

KONTAKT

Für weiterführende Informationen kontaktieren Sie uns.

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE
Zanderstraße 5
53177 Bad Godesberg
www.fkie.fraunhofer.de/cad

Ansprechpartner
Herr Dr. Elmar Padilla
Telefon +49 228 50212-595
elmar.padilla@fkie.fraunhofer.de

SICHERHEIT FÜR DEN CYBERRAUM

Bei der Analyse und Bekämpfung existierender Cyberrisiken leistet das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE als Partner einen wesentlichen Beitrag zur gesamtstaatlichen Cybersicherheit, um eine erfolgreiche Digitalisierung von Staat, Wirtschaft und Gesellschaft zu sichern und zu gewährleisten.

»AVALANCHE« – Ermittlern gelingt Schlag gegen organisierte Cyberkriminalität

Mit der Zerschlagung der Botnet-Infrastruktur »Avalanche« ist nach vierjähriger Ermittlungsarbeit einem internationalen Team ein wichtiger Schlag gegen die organisierte Cyberkriminalität gelungen. »Avalanche« galt als die weltweit größte Infrastruktur zum Betrieb sogenannter Botnetze und hat über mehrere Jahre hunderttausendfach private und geschäftliche Computersysteme und Mobilgeräte mit unterschiedlicher Schadsoftware infiziert. Pro Woche wurden mehr als eine Million Spam- oder Phishing-Mails mit schädigendem Anhang oder Link versendet. Dadurch hat die kriminelle Vernetzung in den vergangenen Jahren durch die mehr als 20 unter »Avalanche« vereinten Botnetze Schäden in Millionenhöhe angerichtet. Bundesinnenminister Thomas de Maizière bezeichnete die Zerschlagung von »Avalanche« als »Kampfansage an die internationale Kriminalität im Cyberraum«.

Bei der Zerstörung dieser komplexen Infrastruktur kamen verschiedene Bausteine parallel zum Einsatz, die erstmals eine solch konzertierte Aktion gegen ein weltweit agierendes Botnetz-System ermöglicht haben. Fraunhofer FKIE hat durch technische Unterstützung im Rahmen eines vom BSI beauftragten Projekts entscheidend zu der Zerschlagung von »Avalanche« beigetragen. Neben der Analyse und massiven Störung der Strukturen von »Avalanche« sowie der Identifizierung der einzelnen Server auf Führungsebene als ersten Schritten stand die Identifizierung und Sicherstellung der Täter im Vordergrund, um diese strafrechtlich zu verfolgen. Dank der Analyse der Schadsoftware konnten über verschiedene durch das FKIE entwickelte Systeme die Opfer der Cyberangriffe identifiziert und benachrichtigt werden. Diese Kontaktmöglichkeit über die Provider führte als Teil der Schadensabwehrstrategie zur Bereinigung der infizierten Nutzersysteme. Aber nur über den Informationsweg: Die endgültige Bereinigung der betroffenen Computer liegt in den Händen der Nutzer.

WAS SIND BOTNETZE?

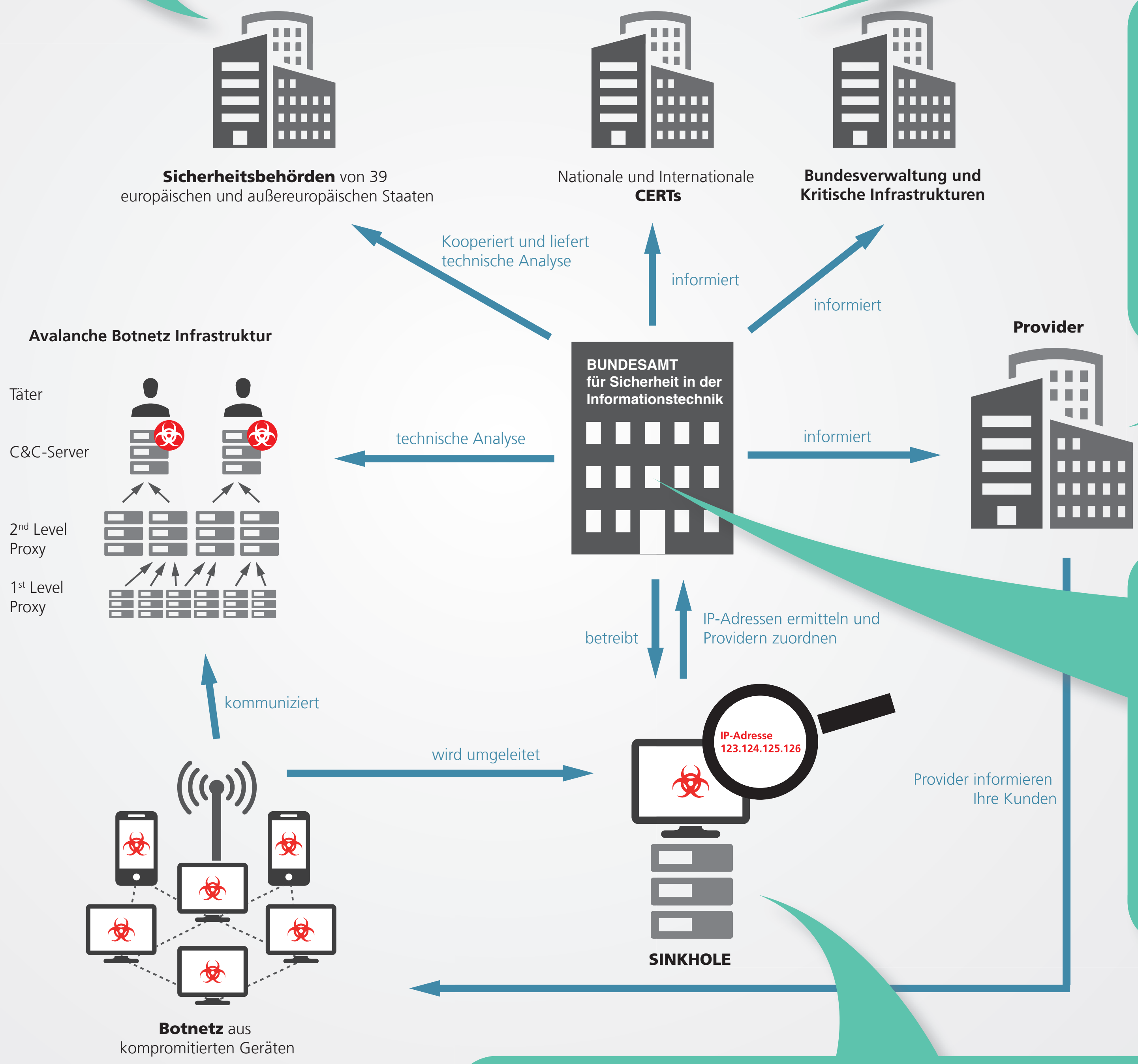
Botnetz ist der Name für eine Gruppe von automatisierten Computerprogrammen, die ein Angreifer aus der Ferne kontrollieren kann. Dabei wird eine Schadsoftware genutzt, um möglichst viele Computer, Smartphones oder Tablets zu infizieren. Betreiber illegaler Botnetze installieren die Bots ohne Wissen der Inhaber auf Computern und missbrauchen letztere für ihre illegalen Zwecke. Die meisten Bots können von einem Botnetz-Operator über einen Kommunikationskanal überwacht werden und Befehle empfangen. Der Betroffene merkt dabei zumeist nicht, dass sein Computer Teil eines Botnetzes ist.

FKIE – ANALYSE DER INFRASTRUKTUR UND SCHADSOFTWARE

Um »Avalanche« zu enttarnen, unterstützte das FKIE die Ermittlungsarbeit **maßgeblich** durch die **technische Analyse der Schadsoftware**. Beteiligt waren an der Aktion neben dem BSI die Staatsanwaltschaft Verden und die Zentrale Kriminalinspektion Lüneburg. Im Laufe der Ermittlungen erweiterte sich der Kreis der Teilnehmer um Mitarbeiter des BKA, des FBI, von EUROPOL sowie von Sicherheitsbehörden aus 39 europäischen und außereuropäischen Staaten.

FKIE – EXTRAKTION VON OPFERDATEN

Im Auftrag des BSI hat das FKIE schon während der Ermittlungen die betroffenen Opferdaten extrahiert und **in einem bestimmten Format abgelegt**. Diese Information wurde dann an CERT-Bund weitergeleitet. CERT-Bund hat daraufhin andere CERTs, die Bundesverwaltung und Kritische Infrastrukturen informiert und die Daten an die jeweiligen Stellen verteilt.



FKIE – SOFTWARE »PI«

Um die Nutzer vor einem Cyberangriff zu warnen, wurde von der Abteilung CA&D des FKIE das **Providerinformationssystem** (PI) entwickelt. Über diese Software werden Opferdaten extrahiert. FKIE leitet im Auftrag des BSI entsprechend Mitteilungen über infizierte Systeme an deutsche Provider weiter, die ihrerseits ihre Kunden über den Angriff informieren. **Seit 2014** wurden so **mehr als 4,5 Millionen Meldungen** an deutsche Provider gesendet.

FKIE – PROJEKT »SYSTEMATISCHE ANALYSE VON BOTNETZEN«

Das FKIE arbeitet seit 2012 bereits erfolgreich über verschiedene Projekte verbunden mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen. Der Beitrag des FKIE an dieser konkreten Aktion lag vor allem in der **technischen und systematischen Analyse** der Botnetz-Infrastruktur und ihrer Schadsoftware sowie in der **Entwicklung von erfolgreichen Resilienzmaßnahmen**.

FKIE – SINKHOLE-SERVER

Mit Hilfe der **vom FKIE entwickelten Sinkhole-Software** werden **Verbindungsanfragen** von auch nach der Zerschlagung von »Avalanche« weiterhin infizierten Systemen auf Sinkhole-Server **weitergeleitet**. Auf diese Weise können die Opfer identifiziert und gewarnt werden.