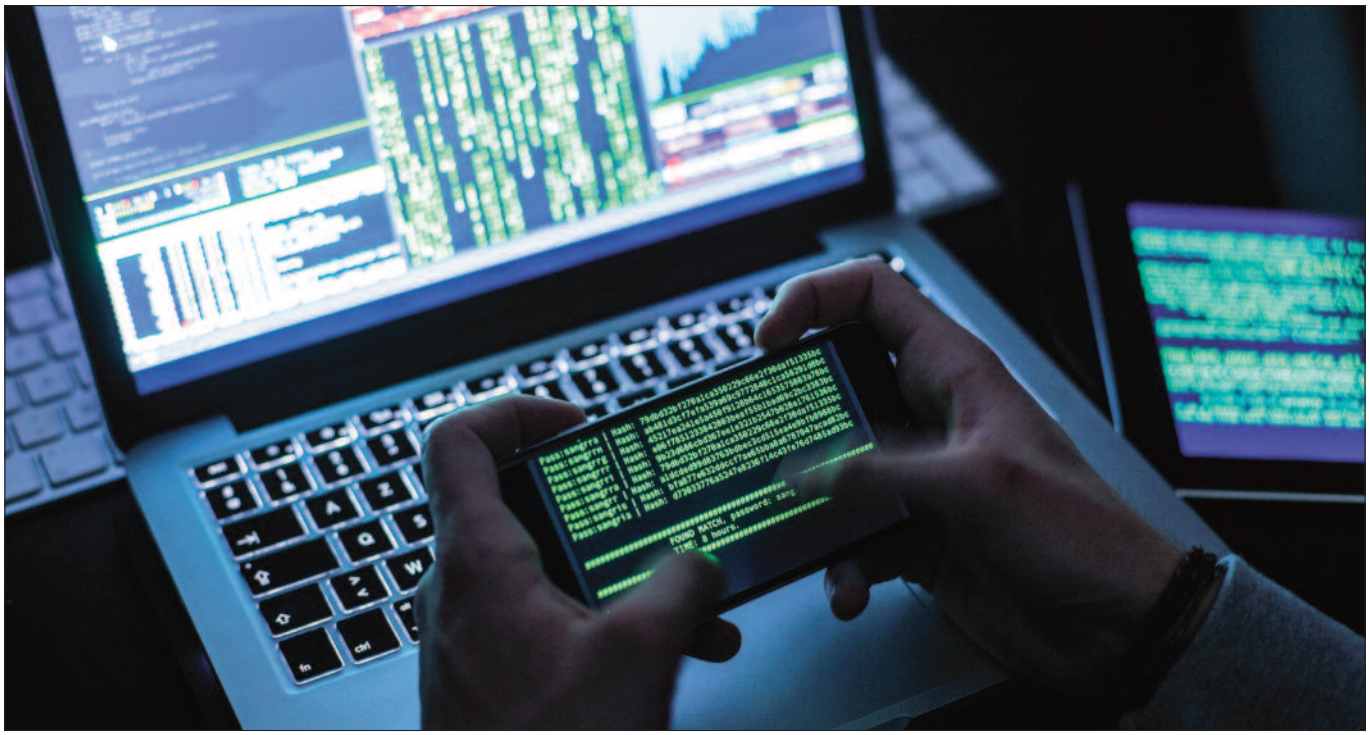

Die Zahl der Hackerangriffe durch vigilante Hacker wird zunehmen – vorgeblich „zum Wohle der Allgemeinheit".

Sabotage, Spionage, Angriffe

Angriffe unter falscher Flagge, Finanzangriffe und Cyber-Spionage werden 2017 laut Experten des Cyber-Sicherheitsunternehmens *Kaspersky Lab* und des *Global Research & Analysis Teams (GReAT)* zunehmen.

Experten des Cyber-Sicherheitsunternehmens *Kaspersky Lab* und des *Global Research & Analysis Teams (GReAT)* rechnen für 2017 mit einer Zunahme von Cyber-Sabotage bei Unternehmen der kritischen Infrastruktur sowie von Spionage auf mobilen Geräten, da immer mehr Nutzer ihre persönlichen Daten auf Smartphones gespeichert haben.

Die Prognosen für 2017 befassen sich unter anderem mit den Auswirkungen maßgeschneiderter und frei verfügbarer Tools bei Cyber-Angriffen, der Verschleierung der Identität bei Angriffen unter falscher Flagge, Sicherheitsproblemen im Internet der Dinge sowie der Nutzung von Cyber-Waffen bei einem Informationskrieg.

Verschleierung. Die Cyber-Sicherheitsexperten erwarten für 2017 eine Zunahme von Malware, die sich nach einem Neustart von selbst aus dem Arbeitsspeicher löscht. Eine solche Malware, die für Spionage und für das Sammeln von Anmeldeinformationen bestimmt sein kann, wird von verdeckt operierenden Angreifern verwendet. Mit ihrer selbstständigen Löschung kann die Entdeckung des Angriffs verhindert werden.

Hacking. Das Hacken und Verbreiten von Daten durch vigilante Hacker wird zunehmen – vorgeblich „zum Wohle der Allgemeinheit". Internet-Vigilantismus ist eine radikale Form des Online-Aktivismus.

Da Hersteller im Bereich des Internets der Dinge weiterhin ungesicherte Geräte ausliefern, die weitreichende Sicherheitsprobleme verursachen, besteht die Gefahr, dass vigilante Hacker diesen Umstand ausnutzen und Geräte deaktivieren, beschädigen oder stören.

Unter falscher Flagge. Cyber-Angriffe spielen eine immer größere Rolle bei internationalen Konflikten. Bei Angriffen auf Cyber-Einrichtungen eines Staates wird vorgetäuscht, dass der Angriff von einer Einrichtung eines anderen Staates erfolgt sei, um einen Konflikt herbeizuführen. In internationalen Beziehungen wird die Zuordnung solcher Angriffe ein zentrales Thema bei der Festlegung politischer Handlungsprozesse sein – beispielsweise bei einer Vergeltungsaktion.

Finanzangriffe. Immer mehr Banken werden von Hackern über das internationale Zahlungsnetzwerk Swift bestohlen. Jeden Tag schicken die Finanzinstitute über das System mehrere Millionen Nachrichten hin und her, mit denen sie grenzüberschreitende Zahlungsaufträge auslösen. Kriminellen gelingt es immer wieder, in die Computersysteme Einzelner an das Netz angebundener Institute einzudringen und sie über Schadsoftware zu manipulieren, dass sie gefälschte Versionen solcher Zahlungsaufträge im Namen der Bank an andere Häuser verschicken können.

Um einen derartigen „Banküberfall" durchzuführen, benötigt man spezialisierte Software, Geduld und eine Geldwäschestruktur. Jeder dieser Schritte wird von Kriminellen ausgeführt, die ihre Dienstleistungen gegen ein Honorar liefern.

Kaspersky-Lab-Experten erwarten eine Kommerzialisierung dieser Angriffe durch spezialisierte Ressourcen, die in Untergrundforen zum Verkauf oder nach dem Schema *As-a-Service* angeboten werden.

FOTO: REPORTERS/PICTUREDESK.COM