Cybersicherheit 2015: Das erwartet uns im nächsten Jahr

Von James Lyne, Global Head of Security Research, Sophos

Cybersicherheit ist eines der am schnellsten wachsenden und sich weiter entwickelnden IT-Themen. Sowohl in der Industrie als auch im täglichen Leben aller Leute, die moderne Technologien nutzen. Und genau diese Technologien verändern sich in einem so atemberaubenden Tempo, dass auch die IT-Sicherheitsgefahren sich ständig wandeln und neue Blüten treiben. Im Folgenden die 10 Top-Trends, mit denen sich IT-Administratoren im kommenden Jahr auseinander setzen müssen:

1. Exploit-Bekämpfung reduziert die Einfallstore für Kriminelle.
Cyberkriminelle hatten in den vergangenen Jahren mehr oder weniger leichtes Spiel mit Microsoft Windows. Glücklicherweise hat der Konzern Exploits in letzter Zeit gezielt bekämpft, so dass Attacken immer schwieriger werden. Allerdings gibt es eine Kehrseite der Medaille, da viele Malwareentwickler sich nun wieder den Social-Engineering-Techniken zuwenden oder auf Nicht-Microsoft-Plattformen abzielen.

2. Internet-of-Things-Attacken haben sich von Machbarkeitsstudien zu Mainstream-Risiken entwickelt.
2014 mussten wir immer häufiger feststellen, dass Hersteller von Internet-of-Things-Geräten es oftmals verschlafen haben, grundlegende Sicherheitsstandards zu implementieren. Entsprechend sind Attacken auf diese Geräte absehbar und werden zudem umfassende Folgen haben. Die IT-Sicherheitsindustrie muss sich weiterentwickeln, um für dieses neue Thema Antworten zu finden.

3. Verschlüsselung ist mittlerweile Standard, aber darüber sind nicht alle glücklich.
Dank häufig auftauchender Schlagzeilen in Sachen Spionagesoftware und Datenbankeinbrüchen hat sich die Verschlüsselung aller Daten schon fast zum Standard entwickelt. Das geht allerdings gerade großen Organisationen wie Strafverfolgungsbehörden oder Geheimdiensten gegen den Strich, da sie befürchten, dass diese „Heimlichtuerei“ die allgemeine Sicherheit gefährdet.

4. Sicherheitsrelevante Programmierfehler in weit verbreiteter Software blieben jahrelang unter dem Radar.
„Heartbleed“ und „Shellshock” machen deutlich, dass weit mehr unsichere Code-Zeilen im Umlauf sind, als gedacht und sie werden seit vielen Jahren unbemerkt von einer großen Anzahl Computersystemen genutzt,. Entsprechend hat sich auch das Augenmerk der Hacker auf diese eher unauffälligen Programme gerichtet und 2015 sind vermehrt Attacken in diesem Bereich zu erwarten.

5. Gesetzliche Neuregelungen bringen mehr Verantwortung bei der Offenlegung von Daten und Haftung mit sich – vor allem in Europa.
Die Mühlen der Gesetze mahlen im Vergleich zur Technologieentwicklung sehr langsam, aber dennoch treten 2015 einige gesetzliche Neuerungen in Kraft, die lange auf sich warten ließen. Es ist wahrscheinlich, dass diese Änderungen auch in anderen Bereichen mit einer progressiveren Datenschutzregulierung einhergehen.

6. Kriminelle schießen sich auf mobile Zahlungssysteme ein, halten aber gleichzeitig noch eine Weile an traditionellen Finanzbetrügereien fest.
Nach der Ankündigung von Apple Pay waren mobile Zahlungssysteme eines der Topthemen der vergangenen Monate. Wie immer, wenn neue Systeme an den Start gehen, werden die Cyberkriminellen nach Lücken Ausschau halten. Da das aber aufgrund einiger sehr positiver Absicherungen nicht ganz einfach sein wird, dürfen wir davon ausgehen, dass die klassischen Onlinegaunereien mit Kreditkarten noch eine Weile weitergehen. Sie sind das bei weitem einfacherer für Betrug zu nutzen.

7. Die Lücke zwischen Sicherheitsaufgaben und geschultem Personal klafft immer weiter auseinander.
Im gleichen Rahmen, wie Technologie immer mehr in unser tägliches Leben Einzug hält und einer der Stützpfeiler für die globale Wirtschaft wird, kommt das fehlende Know-how in Sachen Cybersicherheit zum Vorschein. Diese bedenkliche Entwicklung wird sowohl von Regierungen, als auch der Industrie konstatiert. Das Besetzen der nötigen Stellen kann Jahre dauern und ist somit ein echter Sicherheitsfaktor.

8. Breite "Serviceoffensive" für Attacken und Exploit-Kits, um mobile Plattformen anzugreifen.
In den letzten Jahren hat sich ein neuer Trend bei den Cyberkriminellen durchgesetzt: das zur Verfügung stellen von Malwarepaketen, die keinerlei technisches Wissen voraussetzen und per Klick aktiviert werden können. Der rasante Anstieg bei mobilen Plattformen und der damit verbundene Austausch sensitiver Daten werden dazu führen, dass wir 2015 viele dieser Kits für Smartphone-Angriffe sehen werden. Gleiches gilt für Plattformen, die sich mit dem Internet of Things beschäftigen.

9. Die Lücke zwischen ICS/SCADA und Sicherheit in der realen Welt wächst weiter.
Systeme wie Industrial Control Systems (ICS) und Supervisory Control and Data Acquisition (SCADA) hinken in Sachen Sicherheit üblicherweise zehn oder mehr Jahre hinter dem Mainstream her. Wir gehen davon aus, dass innerhalb der nächsten Jahre einige besorgniserregende Lücken aufgedeckt werden, die von Hackern auf breiter Front ausgenutzt werden.

10. Flexiblere Rootkit- und Bot-Fähigkeiten eröffnen neue Angriffsvektoren.
Die Technologiesparte befindet sich zurzeit in einem grundlegenden Veränderungsprozess, in dessen Rahmen nun Plattformen und Protokolle abgeändert werden, die jahrelang als Standard dienten. Allein die Menge solcher Veränderungen der althergebrachten Technologiestandards wird viele alte Wunden aufreißen und neue Sicherheitslücken schaffen.

Der komplette Report (z.Z. nur in Englisch) steht hier zur Verfügung. Das PDF informiert noch einmal detaillierter über die zehn soeben angesprochenen Trends und gibt weitere Einsichten in das Thema IT-Sicherheit 2015.

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, +49-40-484434
sophos@tc-communications.de