SOPHOS
Security made simple.

Trends für 2014

Von den SophosLabs

Wichtige technologische Entwicklungen sowie eine Reihe von Enthüllungen über die NSA machten 2013 zu einem interessanten Jahr für Trend-Beobachter. In unserer Zusammenfassung der Entwicklungen 2013 haben wir einige Trends herausgegriffen, die wir wahrscheinlich auch im nächsten Jahr beobachten werden.

1. Angriffe auf Unternehmensdaten und private Daten in der Cloud

Da Unternehmen zunehmend Cloud-Dienste nutzen, um Kundendaten, interne Projektpläne und Vermögenswerte zu verwalten, rechnen wir mit einer Zunahme von Angriffen auf Endpoints, mobile Geräte und Anmeldeinformationen. Ziel dieser Angriffe ist es, Zugriff auf Clouds von Unternehmen oder Privatpersonen zu erhalten.

Es lässt sich schwer vorhersagen, in welcher Form zukünftige Angriffe auftreten werden. Allerdings können wir uns Ransomware vorstellen, die Sie nicht nur aus Ihren lokal gespeicherten Dokumenten aussperrt, sondern auch von allen möglichen Daten, die in der Cloud gespeichert sind. Diese Angriffe erfordern nicht unbedingt eine Datenverschlüsselung und könnten in Form von Erpressungen auftreten, d. h. als Drohungen, Ihre vertraulichen Daten zu veröffentlichen.

Strenge Richtlinien für den Einsatz von Passwörtern und für den Zugriff auf Daten in der Cloud sind wichtiger als je zuvor. Sie sind immer nur so sicher, wie es Ihre größte Schwachstelle ist. Diese Schwachstelle dürfte in vielen Fällen Ihr Windows-Endpoint und das Sicherheitsbewusstsein Ihrer Benutzer sein.

2. APTs treffen auf Finanz-Malware

Advanced Persistent Threats sind sehr erfolgreich beim Ausführen von Angriffen, die zur Industriespionage dienen. Wir gehen davon aus, dass dieser Erfolg andere Gruppen anspornen wird, diese Techniken ebenfalls anzuwenden. Interessant könnte dies z. B. für Gruppen sein, die bisher mit weniger ausgefeilter Finanz-Malware arbeiten. Schon jetzt beobachten wir, dass Exploit-Techniken von APT-Gruppen genutzt werden, um Malware zu verbreiten.

Da Sicherheitsanbieter immer effektivere Abwehrmechanismen entwickeln, Betriebssysteme sicherer werden und das Sicherheitsbewusstsein der Benutzer steigt, wird es für Cyberkriminelle immer schwieriger. Sie müssen höhere finanzielle Gewinne von einer kleineren Anzahl Opfer erzielen. Neue Angriffe, die von Betreibern gewöhnlicher Malware angestoßen werden, könnten künftig Komponenten und Bereitstellungsmechanismen enthalten, die noch genauer auf eine ganz spezifische Zielgruppe ausgerichtet sind. Die Grenze zwischen APT und gewöhnlicher Malware wird 2014 weiterhin verschwimmen.

3. Android-Malware: Zunehmend komplex und auf der Suche nach neuen Zielen

2013 konnten wir einen enormen Zuwachs an Android-Malware verzeichnen, nicht nur gemessen an der Zahl einzelner Familien und Versionen, sondern auch an der Zahl der weltweit betroffenen Geräte.

Zwar gehen wir davon aus, dass sich die neuen Android-Sicherheitsfunktionen mit der Zeit positiv auf die Infizierungsrate auswirken werden. Allerdings wird es eine Weile dauern, bis diese Funktionen greifen, und bis dahin bleiben die meisten Benutzer ohne Schutz gegen einfache Social-Engineering-Angriffe. Cyberkriminelle auch weiterhin nach neuen Methoden suchen, um mit Android-Malware Geld zu verdienen. Auch wenn Angreifer auf dieser Plattform weniger Möglichkeiten haben als auf Windows, so bieten mobile Geräte doch eine attraktive Ausgangsbasis für Angriffe, deren Ziel soziale Netzwerke und Cloud-Plattformen sind.

Dämmen Sie das Risiko ein, indem Sie eine BYOD-Richtlinie durchsetzen, die das Side-Loading mobiler Apps aus unbekannten Quellen verhindert und einen Malware-Schutz vorschreibt.

4. Malware wird vielfältiger und spezialisierter

Finanz-Malware stellt sich immer stärker auf Unterschiede ein, die zwischen verschiedenen geografischen und ökonomischen Regionen bestehen. Dies zeigt sich an länderspezifischen Social-Engineering-Techniken, verschiedenen Möglichkeiten, die genutzt werden, um Geld zu erbeuten, sowie an den unterschiedlichen Zielsetzungen der Angriffe. Malware, die in vielfältigen Variationen für unterschiedliche Zielgruppen auftritt, wird 2014 vermutlich weiter zunehmen. insbesondere, um zwischen privaten und geschäftlichen Nutzern zu unterscheiden. Außerdem wird es wohl Angriffe geben, die sich dahingehend spezialisieren, dass sie unterschiedliche Sicherheitslevel und die unterschiedlich hohen Werte der anvisierten Ziele berücksichtigen.

5. Gefahr für persönliche Daten durch mobile Apps und soziale Netzwerke

Die Sicherheit mobiler Geräte wird auch 2014 ein wichtiges Thema bleiben. Da immer wieder neue Apps für die private und geschäftliche Kommunikation genutzt werden, vergrößert sich die Angriffsfläche ständig. Dies gilt insbesondere für Social-Engineering-Scams und für Versuche, Daten zu stehlen. Ihr Adressbuch und Ihre sozialen Netzwerke sind ein wahrer Schatz für Cyberkriminelle. Überlegen Sie sich deshalb gut, wem Sie Zugriff gewähren und warum. Mit Lösungen, die geschäftlichen Nutzern Schutz für mobile Geräte und Webanwendungen bieten, lässt sich das Risiko deutlich minimieren.

6. Neue Waffen gegen Schutzmechanismen

Im niemals endenden Kampf zwischen Cyberkriminellen und Sicherheitsanbietern werden neue Waffen zum Einsatz kommen, die auf die neuesten Mechanismen der Cyber-Verteidigung gerichtet sind. Reputationsdienste, Cloud Security-Datenbanken, Whitelisting und Sandboxing werden neuartigen, gefährlichen Angriffen ausgesetzt sein. Außerdem wird es eine Zunahme geben bei Malware mit gestohlenen digitalen Signaturen, Versuchen, Sicherheitsdaten und telemetrische Analysen zu manipulieren, neuen Techniken, um Sandboxing zu erkennen und zu umgehen, sowie bei der Nutzung seriöser Tools zu schädlichen Zwecken.

7. 64-Bit-Malware

Wegen der zunehmenden Verbreitung von 64-Bit-Betriebssystemen auf PCs rechnen wir mit mehr Malware, die nicht auf 32-Bit-PCs ausgeführt werden kann.

8. Exploit-Kits weiterhin die Hauptbedrohung für Windows

Zwar hat Microsoft bei seinem Windows-Betriebssystem technologische Fortschritte gemacht, mit denen es für Exploit-Entwickler deutlich schwerer wird. Doch das Unternehmen hat den Kampf noch nicht gewonnen.

Mit dem Ende des Supports für Windows XP nach 12 Jahren wird das Betriebssystem ein lukratives Ziel für Angreifer. Wird sich Windows 7 genauso viele Jahre halten können wie XP? Wie lange wird es dauern, bis die Mehrheit aller Endpoints auf neuere Windows-Versionen mit verbesserten Sicherheitsfunktionen migriert?

Bedrohungen, die eine Interaktion der Benutzer erfordern (Social Engineering) werden weiterhin eine Hauptquelle für Infektionen sein. Doch Malware-Autoren werden ihre Techniken verfeinern müssen, um die Benutzer zur Ausführung der Payloads zu bringen, da die Anwender immer besser lernen, zwischen schädlichen und harmlosen Inhalten zu unterscheiden. Autoren von Massen-Malware stehen daher vor der Herausforderung, ihre Köder gezielter und überzeugender zu gestalten.

9. Angriffe auf zentrale Hardware, Software und Infrastrukturen

Die Enthüllungen im Jahr 2013 über Spionage-Angriffe und den Einsatz von Backdoors durch Regierungsbehörden (und auch durch kommerzielle Organisationen) zeigten der Welt, dass Angriffe auf die zentrale Infrastruktur, die uns alle betrifft, nicht nur möglich sind, sondern auch tatsächlich stattfinden. Wir werden neu bewerten müssen, wie sicher unsere Technologien sind und wem wir vertrauen können.

Die bekannt gewordenen Vorfälle sind jedoch nur die Spitze des Eisbergs, und wir können uns 2014 sicherlich auf viele weitere Geschichten dieser Art gefasst machen. Die meisten Unternehmen werden nicht über die Ressourcen oder das Know-how verfügen, nach Backdoors zu suchen. Doch es empfiehlt sich, die Arbeit der Sicherheitsexperten und der Medien aufmerksam zu verfolgen, was neue Enthüllungen angeht.

10. Vor Hackern ist nichts mehr sicher

Wir nutzen immer mehr unterschiedliche Geräte, auf denen oft auch sensible Unternehmensdaten gespeichert sind. Die Sicherheitssysteme dieser Geräte sind einfach noch nicht so gut wie die einer traditionellen PC-Umgebung.

Für diejenigen, die uns Schaden zufügen möchten, sind die eingebetteten Geräte bei uns zu Hause, in unseren Büros und sogar in Städten interessante Angriffsziele. Und da es neue elektronische Währungen und Zahlungstechniken gibt, sollten wir nicht nur unsere Kreditkarten gut im Auge behalten.

Wir erwarten zwar nicht, dass sich Angriffe gegen das „Internet der Dinge“ 2014 sehr weit ausbreiten werden, doch wir rechnen mit mehr Berichten über Schwachstellen und mehr Proof-of-Concept-Exploits.

Download Security Threat Report 2014

sophos.com/threatreport

Sales DACH (Deutschland, Österreich, Schweiz)
Tel: +49 (0) 611 5858-0 | +49 (0)721 255 16-0
E-Mail: sales@sophos.de

Oxford (Royaume-Uni) | Boston (États-Unis)

1091-11.13DD.na.simple

SOPHOS