SOPHOS

Kriminelle im digitalen Untergrund:

Hackertypen und ihre Fähigkeiten

Cyberkriminelle halten die Welt in Atem und aufgrund der guten Verdienst- und schlechten Arrestquoten werden ihre Aktivitäten uns auch künftig beschäftigen. Eine Verteidigung gestaltet sich schwierig und Privatpersonen ebenso wie Unternehmen beobachten nervös, welche Form der Malware und des Datendiebstahls als nächstes die Schlagzeilen füllt.

Sophos stellt die wichtigsten Hackertypen vor, beschreibt ihre Motive und Fähigkeiten und empfiehlt Maßnahmen zum Schutz.

Autor: Michael Veit, Sicherheitsexperte bei Sophos, 11. Oktober 2016

Die Liste der Stichworte ist lang wenn es darum geht, die vielen digitalen Gefahren aufzulisten, die Unternehmen aktuell drohen. Daten werden gestohlen, um sie dann auf den Verkaufstresen des Dark Webs anzubieten oder um sie für erpresserische Zwecke zu verwenden. Kriminelle schleichen sich in Unternehmensnetzwerke um dort entweder alles lahm zu legen, oder heimlich, still und leise über einen langen Zeitraum Daten auszulesen. Staaten bezichtigen sich gegenseitig der Duldung und der Unterstützung von schlagkräftigen Hackerteams, damit diese unerwünschte Parteien oder Organisationen im In- und Ausland ins Visier nehmen und ihnen größtmöglichen Schaden zufügen.

In einem Punkt herrscht allerdings Einigkeit: Es werden Hacker gesucht.

Hacker – verzweifelt gesucht.

Hacker werden weltweit gesucht – sei es, um kriminelle Handlungen zu begehen oder um sie zu verhindern. Denn der Begriff „Hacker“ ist im Bewusstsein der Öffentlichkeit zwar zunehmend negativ besetzt, eigentlich handelt es sich jedoch um einen Computerexperten. Er überprüft Netzwerke, Programme und Systeme, um sie bei Bedarf zu verbessern. Dieser „gute“ Hackertyp – Fachleute reden auch von White-Hats oder Ethical Hacking – ist rechtschaffend und gesetzestreu und wird daher in der folgenden Typisierung nicht berücksichtigt.

Black-Hats, also die Mitglieder der Hackergruppe mit unethischen oder kriminellen Absichten, unterscheiden sich in ihren Motiven und Fachkenntnissen und auch bei der Wahl ihrer Kooperationspartner oder Auftraggeber stark voneinander. Die vier, in Unternehmensnetzwerken am häufigsten anzutreffenden Hackertypen möchten wir Ihnen vorstellen.

1. Der Hacktivist

Der Cyber-Aktivist oder auch Hacktivist nutzt Computer und Computernetzwerke als Protestmittel, um seine Meinung zu verbreiten, bestimmte Missstände aufzuzeigen oder manchmal auch Forderungen durchzusetzen.

Fähigkeiten

Die meisten Hacktivisten verfügen über wenig Technikwissen. Ihnen geht es hauptsächlich um die Botschaft und wie sie diese im und durch das Netz verbreiten können.

Motiv

Zwar ähnelt die Vorgehensweise des Cyber-Aktivisten der eines Kleinkriminellen, doch ihm geht es nicht um Geld – er hat politische und soziale Motive. Er möchte aufklären und auf Missstände aufmerksam machen.

Techniken

Cyber-Aktivisten nutzen verschiedene Tools und Techniken. Die benötigte Software ist teilweise frei im Internet erhältlich. Zu den Techniken gehören die Veränderung von Startseiten, um der jeweiligen Organisation Schaden zuzufügen (Defacement), DDoS-Attacken, mit denen Webseiten lahmgelegt werden, oder Spam-Attacken.

Schutz

Jede zwingend erforderliche Maßnahme zum Schutz der IT-Systeme.

2. Der Wirtschaftsspion

Der Hacker des Typs Spion ist ein Wirtschafts- bzw. APT-Hacker. Bei APTs (Advanced Persistent Threats) handelt es sich um gezielte Angriffe auf eine bestimmte Firma, Gruppe oder Branche. Dabei versuchen die Angreifer ins Netzwerk zu gelangen und sich im nächsten Schritt weiter im Netzwerk vorzuarbeiten. Ziel ist es, dort auf Systeme zuzugreifen, auf denen wertvolle Daten gespeichert sind, z. B. auf Computer von IT-Administratoren oder Führungskräften mit weitreichenden Zugangsberechtigungen. Diese Angreifer verhalten sich ruhig, denn der Angriff soll unbemerkt vonstattengehen.. APTs spionieren das befallene System im Verborgenen aus. Diese Nicht-Aktivität kann über Tage, Wochen, Monate oder sogar Jahre hinweg andauern.

Fähigkeiten

Bei APTs kommen die gleichen Techniken zum Einsatz, wie bei herkömmlichen Hacker-Angriffen. Ein gewisses Maß an technischem Know-how muss daher vorausgesetzt werden. Da die Angriffe mit hohem Aufwand durchgeführt werden, gehören bei den Wirtschaftshackern Hartnäckigkeit und Ausdauer zur Grundausstattung. Vor dem eigentlichen Angriff müssen die Angreifer unter Umständen umfassende Recherchearbeit leisten, um Informationen über ihr Ziel

einzuholen. Solche Gruppen von Angreifern sind meist kapitalkräftig und gut organisiert.

Motiv

Bei den APTs geht es vorrangig um Wirtschaftsspionage, manchmal auch um Sabotage. Ziele der Wirtschaftshacker sind das Ausspionieren von Unternehmensdaten, wie Produktunterlagen, Konstruktionszeichnungen oder auch Patentdatenbanken.

Techniken

Bei den meisten Angriffen sind nach wie vor Techniken im Einsatz, die schon seit Jahren bestens bekannt sind – vornehmlich Social Engineering, Phishing-E-Mails, Backdoor Exploits und Drive-by-Downloads. Solche Angriffe sind weder fortgeschritten noch besonders raffiniert, wenn man ihre einzelnen Bestandteile betrachtet, und zielen oft auf das schwächste Glied im Unternehmen: den Benutzer. Was APTs von anderen Angriffen unterscheidet, ist vielmehr die Kombination verschiedener Techniken und die Langfristigkeit bzw. Hartnäckigkeit der Angreifer.

Schutz

Keine einzelne Lösung kann komplett vor APTs schützen. Um eine erfolgreiche Abwehr verschiedener Bedrohungen zu ermöglichen, sollte man stets auf mehrere Schutzschichten setzen. Web-Exploits, Phishing-E-Mails und Remote-Access-Trojaner sind allesamt beliebte Elemente von APTs. Herkömmliche Sicherheitssysteme sind für die Erkennung von Angriffen im Frühstadium und zum Verhindern ihrer weiteren Ausbreitung also nach wie vor wichtig. Auch SIEM-Lösungen oder Netzwerk-Scans dienen der Erkennung von APTs.

3. Der Infrastruktur-Hacker

Der Infrastruktur-Hacker ist ein Saboteur. Er hat es auf die Schwachstellen kritischer Infrastrukturen abgesehen. Viele für Infrastruktur und Versorgung lebensnotwendige Einrichtungen und Unternehmen sind durch Angriffe aus dem Internet leicht verwundbar, da die Anlagen in einer Zeit gebaut wurden, als Angriffe aus dem Internet noch gar keine Rolle spielten. Das Augenmerk der Hacker liegt auf diesen sogenannten kritischen Infrastrukturen. Dazu zählen beispielsweise industrielle Steuerungssysteme, wie sie in Kraftwerken und großen Produktionsstätten zum Einsatz kommen. Die Angriffe haben das Ziel, die Kontrolle über diese Systeme zu erlangen. Dies kann von jedem beliebigen Ort in der Welt geschehen.

Motiv

Im Unterschied zum Wirtschaftshacker hat der Infrastruktur-Hacker ein anderes Hauptmotiv: er will Kontrolle über das System erlangen, um kritische Infrastrukturen zu blockieren oder zumindest zeitweise lahmzulegen.

Techniken

Infrastruktur-Hacker scannen und durchsuchen das Internet ständig nach verwundbaren Systemen. Dafür finden sie unter anderem mit der Google Hacking Database kostenlose Tools im Internet. Für den Angriff verwenden Infrastruktur-Hacker bekannte Angriffstechniken wie SQL Injection oder Spear Phishing. Auch versuchen Hacker Zugriff auf diese Systeme per Brute Force zu bekommen. Hierbei versuchen sie ein Passwort zu knacken, indem eine Software in schneller Abfolge verschiedene Zeichenkombinationen ausprobiert.

Fähigkeiten

Um Zugriff auf Infrastrukturen zu bekommen sind nicht unbedingt tiefere Kenntnisse nötig, denn diese Systeme weisen teilweise erhebliche Sicherheitslücken auf, wie beispielswiese unverschlüsselte Verbindungen, Verwendung von Standardzugangsdaten, die im Internet kursieren, sowie relativ leicht angreifbare Wartungszugänge.

Schutz

Zum Schutz dieser Infrastrukturen empfiehlt sich ein Mix aus verschiedenen Sicherheitstools. Dazu gehören z.B. Intrusion Detection und Intrusion Prevention Systeme (IDS, IPS) und vor allem das sog. Security Monitoring. Hier werden die verschiedenen Logs, die sicherheitsrelevante Informationen enthalten (z.B. Firewall-Logs, Proxy-Logs, Logs von misslungenen Anmeldeversuchen), zusammengeführt um ungewöhnliche Kombinationen von Aktivitäten aufzudecken. Wichtig zum Schutz ist auch die Aufteilung des Netzes in verschiedene Segmente, die sowohl gegeneinander als auch bei der Anbindung an das Internet abgesichert werden müssen.

4. Der Spammer

Spam ist eine unerwünschte E-Mail-Nachricht, die massenhaft und ungezielt verbreitet wird. Werbung ist die harmlose Variante; in schlimmsten Fall enthält die Nachricht aber Schadprogramme im Anhang oder Links zu Webseiten mit Drive-by-Exploits oder wird für Phishing-Angriffe genutzt. Spammer haben aufgrund der großen Gefahr, erwischt zu werden, schon vor Jahren aufgegeben, eigene Spams zu versenden. Heute nutzen die Spammer Bot-Netze (auch Zombies genannt) zum Versenden der Spams. „Bot" steht hier für „Robot", weil private Computer in ferngesteuerte „Cybercrime-Roboter“ verwandelt werden. Das Wort „Zombie" zeigt an, dass ein Cyber-Krimineller diesen Computer ohne Wissen des Besitzers zum Leben erwecken und ihn nach für seine eigenen Zwecke einsetzen kann. Die betroffenen Computer gehören in aller Regel Privatpersonen, die den Missbrauch häufig nicht bemerken.

Fähigkeiten

Je nach Angriffstechnik benötigt der Spammer ein gewisses Maß an technischen Fähigkeiten und Computer Know-how, doch wichtiger für den Erfolg sind wahrscheinlich Kreativität und Phantasie bei der Erstellung der Spams.

Motiv

Steckt hinter der E-Mail die Absicht, an sensible Daten heranzukommen (Phishing-Angriff) dann ist das Motiv rein finanzieller Natur. Sollen lediglich Werbebotschaften verbreitet werden, wobei Auftraggeber meistens Unternehmen sind, die ihre Verkäufe steigern wollen, so ist das Motiv langfristig zwar auch finanzielles Interesse (mehr Verkauf), kann aber auch der Steigerung der Aufmerksamkeit dienen.

Techniken

Neben Bot-Netzen, mit denen Spammer ein ganzes Netz aufbauen können, das mehrere 10.000 Rechner kontrollieren kann, sind vor allem die sogenannten SQL-Injections beliebt. Der Angreifer nutzt dabei Fehler in einer Web-Applikation so aus, dass er Befehle an die dahinterliegende Datenbank senden kann. Auch Denial-of-Service-Angriffe nahmen in den letzten Jahren zu.

Schutz

Da die Mails oft von vermeintlich vertrauenswürdigen Absendern kommen, sollten Nutzer grundsätzlich vorsichtig sein, wenn sie E-Mails oder Anhänge öffnen wollen. Dies sollte niemals geschehen, wenn der Absender unbekannt ist oder nicht eindeutig verifiziert werden kann. Bei der Angabe von Links doch sollte sich der Nutzer stets darüber bewusst sein, dass die Wahrscheinlichkeit besteht, dass die Site mit Schadsoftware behaftet ist. Seriöse Unternehmen fordern niemals dazu auf, den in der E-Mail mitgesendeten Link anzuklicken und seine Kontonummer einzugeben. Weiterhin empfiehlt es sich, eine Sicherheitslösung einzusetzen, die über eine einfache Malware-Erkennung hinausgeht und zudem Funktionen wie Spam-Entdeckung und URL-Blockierung enthält.

Fazit

Die Kenntnisse, Methoden und Organisation der Hacker ist so unterschiedlich, wie ihre Ziele, eine einheitliche Lösung gibt es nicht. Für Privatpersonen liegt der größtmögliche Schutz noch immer in guten, einmaligen Passwörtern und einer Sicherheitssoftware wie etwa Sophos Home.

Um den vielen Facetten des professionellen Hackings gerecht zu werden, hat Sophos die Synchronized Security-Technologie entwickelt. Hier stellt der „Sophos Heartbeat“, das technologische Kommunikationsnetz, eine Verbindung zwischen Endpoints und der Firewall her. Heartbeat übermittelt verdächtiges Verhalten einzelner Geräte oder bösartige Attacken in Echtzeit. Die traditionell bisher getrennt arbeitenden Produkte erhalten nun die Möglichkeit sich auszutauschen und sofortige Aktionen einzuleiten, um einen Malware-Ausbruch oder Datendiebstahl zu unterbinden.

Hacker werden Unternehmen auch in Zukunft in Atem halten – aber vielleicht sind diese dann besser vorbereitet.

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.