Advanced Persistent Threats: die jüngste und gefährlichste Generation der Sicherheitsbedrohung

Die jüngsten Angriffe auf Unternehmens- und Kundendaten bei Sony, Epsilon oder RSA offenbaren eine neue Dimension an Sicherheitsbedrohungen. Hier geht es gezielt um das Ausspionieren von Unternehmen und Behörden. Die Technik, die hinter diesen Angriffen steckt, macht sogar Sicherheitsexperten sprachlos. Ivan Bütler

Die Meldungen sind noch taufrisch: Bei Sony wurden monatelang die Kundendaten von über 100 Millionen Playstation-Spielern ausspioniert, beim Kreditkarten-Abrechnungsunternehmen Epsilon entstand durch Kreditkartenbetrug ein Millionenschaden. Beim Security-Spezialisten RSA wurde eingebrochen und Schlüsseldaten wurden entwendet. Und mit dem Trojaner Stuxnet wurde erstmals die Schwelle von der Spionage zur Sabotage überschritten.

Bis vor kurzem konnte man das Vorgehen bei allen Sicherheitsbedrohungen wie Malware oder Viren als eine Art Schrotflinten-Taktik beschreiben. Der Erfolg dieser Attacken hing einfach von der enormen Verbreitung ab. Selbst minimale «Erfolgsquoten» von Promille-Bruchteilen reichten den Versendern aus, denn die entsprechende Schadsoftware wurde millionen- oder manchmal sogar milliardenfach verschickt. Doch in jüngster Zeit haben sich die Angriffstaktiken gewandelt. Kurz gesagt lautet die neue Strategie: mehr Klasse statt Masse. Das Buzzwort dafür heisst «Advanced Persistent Threats» (APT). Dabei handelt es sich um sehr gezielte Angriffe, die meist nur durch wenige E-Mails ausgelöst werden. Ziel ist entweder Industriespionage oder das unbemerkte Kopieren von bestimmten Daten und neuerdings sogar das Auslösen von Steuerkommandos, um Industrieanlagen zu stören.

Das wichtigste Kriterium für einen APT-Angreifer ist vergleichbar mit einem natürlichen Spion: Er muss mit allen Mitteln versuchen, so lange wie möglich unerkannt zu bleiben, damit er so lange wie möglich Daten liefern oder andere Auftragsaktionen ausführen kann. APT-Software ist also periodisch mit einem Command- und Control-Server verbunden (C&C), an den es die ausspionierten Daten schickt und von dem es neue Kommandos und Software-Updates erhält. Die bekannten Zeiträume dafür variieren zwischen mehrmals täglich bis zu einmal vierteljährlich. Die vom Angreifer gewählten Zeiträume sind ein Kompromiss zwischen der Gefahr, durch die Kontaktaufnahme entdeckt zu werden, und der Notwendigkeit, aktuelle Daten zu erhalten.

Ivan Bütler ist Gründer und CEO von Compass Security AG, eine auf Ethical Hacking und Penetration Testing spezialisierte Firma aus Rapperswil-Jona.

Staaten mischen mit

So unterschiedlich wie die APT-Attacken im Vergleich zu «normalen» Virenangriffen sind, so sehr unterscheiden sich auch die Personen und Methoden hinter den APT-Angriffen. APT-Angreifer sind hochqualifiziert, haben eine tiefe Systemkenntnis über alle bekannten Systemschwachstellen und die verfügbaren Abwehrmassnahmen. Nicht selten stehen Unternehmen oder sogar Staaten hinter den besonders trickreichen APT-Attacken. Trotzdem unterscheidet sich ein APT-Angriff zunächst kaum von einem normalen Spam- und Malware-Angriff, denn auch bei APT erfolgt die ursprüngliche Verbreitung zumeist durch E-Mail. Die besonders clevere Art von APT zeigt sich aber erst darin, wie diese Malware wirkt. So nutzen APT-Angriffe meistens mehrere Schwachstellen gleichzeitig aus, und sie sind gegen die meisten Tools zum Entfernen von Malware immun. Rein statistisch gesehen kann durchschnittlich alle 50 Tage eine Windows-Lücke das Ausspionieren von Administrator-Rechten ermöglichen.

Die Motive der APT-Angreifer sind sehr unterschiedlich. Meist geht es um das Ausspionieren von Finanz- und Kreditkartendaten. Doch auch militärische und/oder politische Daten können das Ziel solcher Attacken sein. Laut Greg Hoglund vom Sicherheitsanbieter HBGary ist APT nur eine hübsche Umschreibung für das Ausspionieren der amerikanischen Regierungsdaten und Militärsysteme. «APT ist die von der chinesischen Regierung gesponserte E-Spionage, die das Land seit 20 Jahren betreibt, um ihren Wachstumskurs beizubehalten», lautet seine etwas drakonische Definition.

Nicht mehr nur Software-, sondern auch Hardwareattacken fordern Experten heraus. Bildquelle: Symantec

Nuklear-Anlagen in Gefahr

Doch dabei hat er nicht ganz Unrecht, denn auch bei dem bislang bekanntesten und gefährlichsten APT-Programm handelte es sich um den Angriff auf Regierungseinrichtungen. Stuxnet hiess der Trojaner, der die Sicherheitsexperten für lange Zeit sprachlos machte. Das Besondere an diesem Programm war nicht so sehr die hochintelligente Programmierung, sondern seine geplante Wirkung, denn Stuxnet war darauf ausgelegt, die Nuklear-Anlagen im Iran zu sabotieren. «Es ist der erste bekannte APT-Angriff, der nicht nur spioniert, sondern zur Sabotage übergegangen ist», sagt Symantecs CTO Mark Bregman über die Form der APT-Bedrohung.

Auch die Funktionsweise von Stuxnet verblüffte die Experten. «Die Programmierer von Stuxnet hatten ganz intime Windows-Kenntnisse, inklusive Einblicke in den Source-Code von bestimmten Modulen, der Trojaner nutzte parallel vier Zero-Day-Windows-Schwachstellen aus», so Bregman über diesen APT-Angriff.

Stuxnet und die meisten anderen APT-Programme verfügen über eine Multifunktionsfähigkeit, die sich vor allem beim Entfernen besonders negativ bemerkbar macht. So versucht das FBI seit Mitte April eines der besonders aggressiven APT-Botnetze zum Erliegen zu bringen. Das unter dem Namen Coreflood bekannte Netz operiert schon seit vielen Jahren. Dabei wird in dem Client eine Software installiert, die unbemerkt Log-in-Daten ausspioniert und diese an ihren C&C-Server verschickt. Experten schätzen, dass es weltweit mindestens zwei Millionen mit Coreflood infizierte PCs gibt.

Gemeinsam mit Microsoft hat man zunächst die C&C-Server und die zugehörigen Domains vom Internet gesperrt, doch das löste das Problem nicht, denn die meisten infizierten PCs suchen weiterhin das Internet nach einem passenden C&C-Server ab. Beim Auftauchen eines solchen Servers würde das APT-Botnetz sofort wieder aktiv werden. Nur mit dem Entfernen der Client-Software auf den PCs kann Coreflood endgültig ausgemerzt werden. Deshalb versucht das FBI, den C&C-Server zu simulieren und von dort aus die gefährliche Client-Software zu löschen – doch das ist nur mit Erlaubnis des PC-Inhabers möglich. Diese Zustimmung muss auch noch schriftlich erfolgen, denn der User muss sich damit einverstanden erklären, dass seine Festplatte durch das Entfernen der Malware möglicherweise komplett gelöscht wird.

Trotzdem ist der Kampf gegen die APT-Attacken nicht hoffnungslos. «Die meisten APT-Programme lassen sich inzwischen mit normalen Security-Patches und System-Upgrades abwehren», sagt Scott McIntyre, Senior-Technologie-Spezialist bei Telstra Security. Seiner Meinung nach ist die Ausbreitung von APT-Angriffen vor allem ein menschliches beziehungsweise ein Management-Problem. «Wer seine Windows- und Office-Systeme stets auf dem neuesten Stand hält, hat wenig zu befürchten, denn die meisten APT-Attacken nutzen lediglich bekannte Schwachstellen aus», lautet sein Hinweis an die System-Administratoren.

Schwachstelle im Flash-Player

Als Beispiel verweist McIntyre auf die skandalträchtige APT-Attacke beim Sicherheitsunternehmen RSA, bei der eine bekannte Schwachstelle im Flash-Player im Zusammenhang mit einer Integration in Microsoft-Excel ausgenutzt wurde. «Der APT-Angriff hat eine alte Version von Excel beziehungsweise Office 2007 ausgenutzt, es wäre überhaupt nichts passiert, hätte RSA inzwischen auf das viel sicherere Office 2010 umgestellt», lautet sein Vorwurf an die Systempflege des Security-Spezialanbieters, der inzwischen nur noch eine Abteilung von EMC ist.

Die Gefahr steigt trotzdem rasant an. So ist die Zahl der bekannten APT-Attacken laut dem jüngsten Sicherheitsbericht von Messagelabs Intelligence gerade in jüngster Zeit deutlich gestiegen. «Wir müssen abwarten, ob es sich bei die aktuellen Zunahmen um absolute oder nur relative Steigerungen handelt», sagt Paul Wood, Senior-Analyst bei Messagelabs Intelligence. Seiner Ansicht nach gibt es Hinweise darauf, dass die APT-Angriffe immer im Frühjahr besonders deutlich ansteigen. «Vermutlich hat es damit zu tun, dass in dieser Zeit die meisten Geschäftsberichte erstellt werden und die Angreifer an den darunterliegenden Daten interessiert sind – aber wir haben derzeit noch nicht genügend abgesichertes statistisches Material, um hier eine Art ‹Saisonbereinigung› durchzuführen», sagt er über den APT-Trend.

Auch das Symantec-Operations-Center in Virginia berichtet von zunehmenden APT-Angriffen in jüngster Zeit. So hat man dort im vergangenen April durchschnittlich 85 APT-Angriffe pro Tag ausgemacht. Das hört sich im Vergleich zu den Milliarden an Spam- und Virenangriffen sehr gering an, doch man muss dazu wissen, dass das nur die Angriffe sind, die Symantec als solche erkannt hat. Wie viele böse Nachrichten unerkannt durchs Netz gerauscht sind, weiss man nicht, doch dürfte die Dunkelziffer um ein Vielfaches höher sein als das, was man derzeit automatisch als APT-Angriff erkennen kann.

Und dann gibt es noch einen zweiten wichtigen Aspekt in diesem Zusammenhang: Ein einziger erfolgreicher APT-Angriff kann einen Schaden im zwei- oder gar dreistelligen Millionenbereich verursachen. Sony, Epsilon und TJMax sind die bekanntesten Beispiele dafür.

Hochgefährliche Hardware-Malware

Diese bislang beschriebenen APT-Attacken beziehen sich aber alle auf softwarebasierte Schwachstellen und Angriffe. Doch darüber hinaus ziehen am Horizont bereits neue Bedrohungspotenziale auf. Beispielsweise häufen sich die Berichte, wonach USB-Laufwerke bereits werkseitig mit vorinstallierter Malware auf den Markt kommen, die unbemerkt bei der Erstbenutzung ein APT-Programm installieren.

Noch gefährlicher als infizierte USB-Laufwerke sind aber Prozessoren, die bereits werkseitig mit Malware ausgeliefert werden. Professor John Villasenor von der University of California meint, dass inzwischen solche Prozessor-Chips im Umlauf sind und dass diese nur auf einen Aktivierungsbefehl warten. Im einfachsten Fall blockieren sie dann die Funktionsfähigkeit des PCs oder des Handys. Doch der wahrscheinlichere Fall ist für Villasenor ein unbemerktes Ausspionieren des gesamten Systems, beispielsweise das Verschicken von E-Mail-Kopien oder Kreditkartendaten an einen geheimen Server. «Bei der Art, wie heute Chips entwickelt werden, ist schon rein statistisch gesehen die Wahrscheinlichkeit für ein unkontrolliertes Design gegeben», lautet seine Hypothese. Dabei bezieht er sich darauf, dass an einem einzigen Chip-Design heute hunderte Unternehmen weltweit beteiligt sind. Insgesamt soll es weltweit 1550 derartiger Design-Firmen geben, die jeweils auf bestimmte Funktionsblöcke eines Prozessors spezialisiert sind. Diese Firmen entwickeln jährlich rund 2500 Chips. «Beim Chip-Design sind wir heute an dem Punkt, an dem vor 15 Jahren das Internet war: Alles basiert auf gegenseitigem Vertrauen, und man kann sich nicht vorstellen, dass auch Leute mit unlauteren Absichten daran beteiligt sein können. Doch je grösser der Teilnehmerkreis wird, umso höher ist die Wahrscheinlichkeit, dass auch Ganoven darin aktiv sind», sagt er über die gegenwärtige Situation der weltweiten Halbleiter-Entwicklung.

Das US-Pentagon hat sich der Sache schon sehr ernsthaft angenommen und befürchtet, dass vielleicht ihre Waffensysteme auf diese Art infiziert sind und bei Bedarf ferngesteuert deaktiviert werden könnten. Um zumindest für die Zukunft gerüstet zu sein, verlangt das Ministerium jetzt eine genaue Angabe von ihren Systemlieferanten, welche Firmen und Personen am Chip-Design beteiligt waren. Nur Personen mit einer entsprechenden US-Sicherheits-Clearance dürfen solche Arbeiten ausführen – egal wo sie auf der Welt arbeiten. <

HACKING DAY 2011 – CYBER CRIME UND CLOUD HACKING

Advanced Persistent Threat ist auch ein Thema am Hacking Day 2011, der am 16. Juni in Zürich stattfindet und von Digicomp und der Information Security Society Switzerland (ISSS) organisiert wird. In einem Workshop wird gezeigt, welche Mechanismen wirken und welche Lehren man heute bereits daraus ziehen kann, um in Zukunft besser vor APT gewappnet zu sein. Ausserdem stellen Experten in diversen Vorträgen und Live-Demos unter anderem Hacking in der Cloud, Cyberspionage und Forensics in virtuellen Umgebungen vor. Anmeldung unter: **www.digicomp.ch/iit/hackingday**

«Bei IT-Security geht es zu wie im Wilden Westen»

Wie einfach es ist, einen Trojaner in ein Computersystem einzuschleusen und was dieser dann anrichten kann, zeigt Ivan Bütler, Gründer und CEO von Compass Security AG, am Hacking Day 11 in Zürich. Im Interview mit der Netzwoche erklärt er, welche Gefahren im Web lauern. Interview: Anja Schütz

Herr Bütler, Sie zeigen in Live-Demos, wie einfach es ist, ein System zu hacken. Im Auftrag von Kunden greift Compass Security deren Computersysteme an, mit dem Ziel, Schwachstellen aufzudecken. Wo liegen die grössten Schwachstellen bei Schweizer Unternehmen?

In letzter Zeit haben wir viel von Sony gehört – hier handelt es sich meines Erachtens um einer der grössten realen Advanced-Persistent-Threats-Angriffe, kurz APT genannt. Und der Stuxnet-Trojaner ist nach wie vor ein grosses Thema. Schweizer Firmen sollten sich besonders gegenüber Wirtschaftskriminalität aus dem Internet schützen, sich laufend über die Gefahren im Netz informieren und proaktiv Anti-Hacker-Massnahmen umsetzen.

Was hat denn Sony Ihrer Meinung nach falsch gemacht? Hat das Unternehmen wirklich bei der Sicherheit seines Systems geschlampt oder kann man eine solche Attacke gar nicht verhindern?

Aus meiner Sicht hat Sony seine Systeme einfach nicht adäquat geschützt. In der Schweiz verlangt das Gesetz, dass ein System entsprechend dem Stand der aktuellen Technik geschützt sein muss. Das war bei Sony sicher nicht der Fall. Ausserdem gehe ich davon aus, dass Sony gegen die PCI-Vorschriften verstossen hat. Jedes Unternehmen, das kritische Daten verwaltet, arbeitet mit den Data-Security-Standards der Payment Card Industry. Diese gibt vor, dass sich jedes Unternehmen auditieren lassen muss.

Dennoch gibt es heute nicht nur softwarebasierte Schwachstellen und Angriffe – eine ernstzunehmende Bedrohung ist auch durch Hardware gegeben.

Das ist richtig, diese sogenannten Hardware-Malware-Bedrohungen häufen sich in letzter Zeit. Bei 99 Prozent aller Unternehmen weltweit geschehen diese Angriffe über USB-Sticks oder andere Hardware, und nur die wenigsten können sich heute davor schützen. Die Hacker suchen nach immer neuen Möglichkeiten, sich unautorisierten Zugang zu verschaffen.

Wie kann sich Unternehmen vor dieser Art Malware schützen?

Ivan Bütler, CEO der Compass Security AG, ist der Meinung, dass Hacker noch viele Jahre relativ leichte Angriffsziele vorfinden werden.

Hier kann sich ein Unternehmen die Sicherheitsmassnahmen von Museen zum Vorbild nehmen. Diese schützen die wertvollen Gemälde vor Diebstahl mit der sogenannten Compartment Security. Man kann sich im Louvre die Mona Lisa zwar anschauen, aber anfassen wäre keine so gute Idee. Das Bild ist durch ein ganzes System von Alarmanlagen geschützt. Man kann zwar nicht verhindern, dass ein möglicher Einbrecher ins Museum hineinkommt, aber hinaus kommt er bestimmt nicht mehr. Und diese Analogie könnte man zukünftig – im Fall des Schutzes vor Hardware-Malware – auch für IT-Security anwenden. Man grenzt damit den Wirkungskreis von bösartigen Programmen ein.

Am 16. Juni führen Sie am Hacking Day in Zürich auch eine Live-Demo vor, was genau bekommt man dort zu sehen, und was wollen Sie den Besuchern vermitteln?

Es ist ein sehr wichtiges Thema, Mitarbeiter in Unternehmen hinsichtlich IT-Security zu sensibilisieren. Heute reicht es nicht aus, technische Hilfsmittel zu haben. Das Personal muss richtig geschult sein, um zu wissen, wie man mit bestimmten Sicherheitsrisiken umgeht. Bei der Live-Demo werde ich zeigen, wie einfach man mit einem USB-Stick einen Trojaner auf ein System bringen und gleichzeitig diesen infizierten Computer ausspionieren kann.

Wie reagieren Ihre Zuschauer, wenn Sie vor deren Augen ihre IT-Systeme knacken?

Viele sind erstaunt, wie einfach man ein Computersystem mit Malware infizieren kann. Bildlich gesprochen sind wir im Wilden Westen und leben noch nicht in der Zivilisation, die richtige «elektronische Hygiene» betreibt. Jeder kann jeden erschiessen und wird dafür kaum zur Rechenschaft gezogen. Der Umgang mit den neuen Medien wird sich ändern, nach dem Hype der Gadgets und unbeschränkten Möglichkeiten wird es eine Zeit der Normalisierung geben.

Wie wird denn die Privatsphäre in 20 Jahren aussehen?

Ich gehe davon aus, dass man das Gesundheitsdossier einer Person online einsehen kann. Dies hat sowohl positive als auch negative Folgen. Positiv betrachtet kann sich ein Patient besser über Heilungsverfahren informieren. Nachteilig könnte sich diese Information bei einer Stellenbewerbung auswirken.

Neben Ihrer Tätigkeit als Geschäftsführer bei Compass Security unterrichten Sie auch an der Hochschule für Technik in Rapperswil und an der Hochschule Luzern. In welchem Rahmen bilden Sie die Studenten aus?

Wir führen eine Sensibilisierung zum Thema Web-Security durch, und das nicht nur in der Theorie, sondern auch in der Praxis. Hierzu gehe ich mit den Studenten in das Hacking-Lab von Compass Security und zeige ihnen dort anhand praktischer Beispiele, wo die Schwachstellen im Web liegen. Die Studenten erhalten dann die Möglichkeit, selbstständig Angriffe und Abwehrmassnahmen zu testen und zu lernen, auf was es letztlich beim Schutz ankommt.

Was sind für Sie heute die grössten Sicherheitsbedrohungen für ein Unternehmen?

Inside-out ist für mich das Hauptproblem, dann kommen noch die mobilen Geräte hinzu, die immer mehr werden, damit steigen jedoch auch die Sicherheitsrisiken in Unternehmen. Ein weiteres Problem ist der Datenverlust über soziale Netzwerke. Tendenziell liegt ein Grundproblem nach wie vor in der Komplexität und im Wandel der Gesellschaft. Hacker werden noch viele Jahre relativ leichte Angriffsziele vorfinden. <