Bild: iStockPhoto

Dossier
Hacking Day 2015

In Kooperation mit **Digicomp**

Kampf gegen Advanced Persistent Threats

mur. Viele Unternehmen wissen nicht, was ein Advanced Persistend Threat ist, obwohl sich auch kleinere und mittelgrosse Firmen vor dieser Gefahr schützen sollten. Dieses Dossier, das in Kooperation mit Digicomp erstellt wurde, klärt auf. Ein Fachbeitrag legt dar, warum ein Angriff nur schwer zu erkennen ist, wie eine solche Attacke überhaupt zustande kommt und was Unternehmen dagegen tun können. Im Interview sprach die Redaktion mit Yves Kraft, Team Leader Bern und Senior Penetration Tester bei der auf ganzheitliche IT-Security-Beratung spezialisierten Oneconsult AG, und Immanuel Willi, Senior Security Consultant & Penetration Tester beim gleichen Unternehmen. Die beiden Sicherheitsspezialisten erzählen unter anderem, was die Besucher am Hacking Day 2015 bei Digicomp erwartet.

Advanced Persistent Threat – warum auch kleine Fische ins Netz gehen

Unter dem Fachbegriff «Advanced Persistent Threat» (zu Deutsch: fortgeschrittene andauernde Bedrohung) wurde in den letzten Jahren eine neue Art von Cyberangriff bekannt. Sogenannte APTs nutzen verschiedenste Methoden und Techniken, um unbemerkt versteckte Angriffe auf ausgewählte Ziele durchzuführen, mit der Idee, langfristige Verbindungen aufrechterhalten zu können. Autoren: Yves Kraft, Immanuel Willi

DIE AUTOREN

Yves Kraft (oben) ist Team Leader Bern, Senior Penetration Tester & Security Consultant und Immanuel Willi (unten) ist Senior Security Consultant & Penetration Tester bei der Oneconsult AG. www.oneconsult.com

Beide Autoren sind Referenten am Hacking Day am 9. September 2015 in Zürich. www.digicomp.ch/hackingday

Der Lebenszyklus eines APT-Angriffs kann in mehrere Phasen und Einzelschritte gegliedert werden. In einer ersten Vorbereitungsphase werden möglichst viele Informationen über das Ziel gesammelt, damit der Angriff systematisch vorbereitet und durchgeführt werden kann. Das Schlüsselelement dabei ist, bei der Infizierung nicht erkannt zu werden. Nach einer erfolgreichen Infizierung finden weitere Phasen der Verteilung und der Persistenz statt. Hierbei werden weitere Systeme im Zielnetzwerk übernommen und der persistente Zugang zum Ziel gesichert. Dazu werden häufig alternative Zugänge mittels Tunneling- und Backdoor-Techniken geschaffen, damit der Zugriff auf die kompromittierten Systeme jederzeit möglich ist. Nun hat der Angreifer die Möglichkeit, über einen längeren Zeitraum Daten zu sammeln oder Systeme gezielt zu manipulieren. Solange der Angriff nicht entdeckt wird, befindet sich der Angreifer im Netzwerk, kann Daten mitlesen und manipulieren.

APT als reale Bedrohung: Stuxnet und «Operation Oil Tanker»

Der Begriff APT wurde im Zusammenhang mit den Angriffen auf das iranische Atomprogramm durch Stuxnet im Jahr 2010 populär. Ursprünglich als Computerwurm bezeichnet, wurde bei der Aufarbeitung des Malwarevorfalls rasch ersichtlich, dass der Angriff über hochkomplexe Elemente verfügt und die Bezeichnung Computerwurm die Malware nicht ausreichend beschreibt: Kompromittiert wurde das SCADA-System der iranischen Urananreicherungsanlage vermutlich durch ein infiziertes Notebook eines Technikers, das zum Programmieren von Siemens-Controllern verwendet wurde. Stuxnet infizierte die Siemens-Controller, die den Betrieb der Zentrifugen steuern. Der eigentliche Angriff auf die Zentrifugen wurde über zwei verschiedene Methoden durchgeführt.

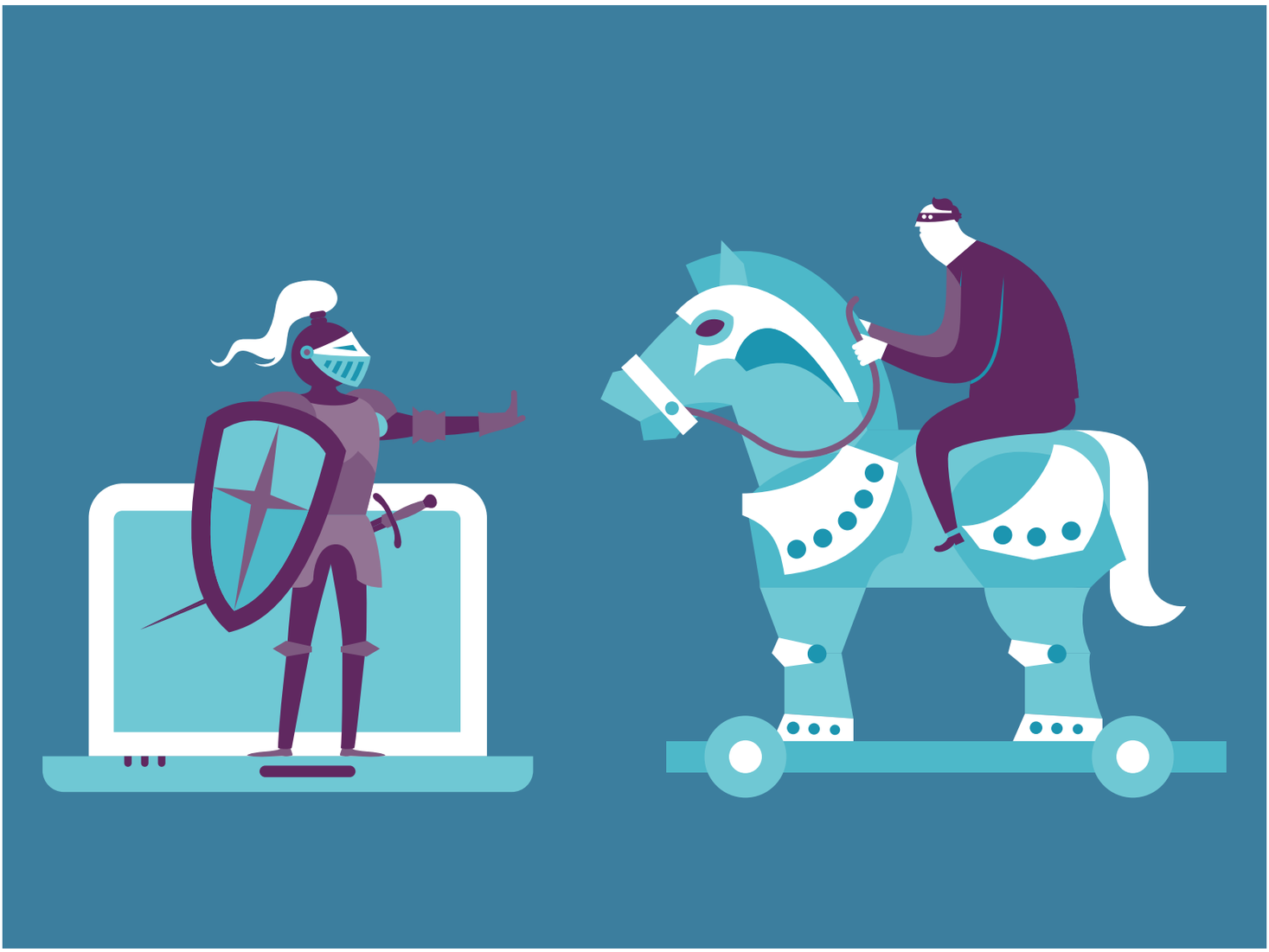
Der erste Angriff erhöhte den Gasdruck innerhalb der Zentrifuge, der zweite die Drehzahl der Rotorenblätter der Zentrifuge. Durch beide Methoden wirkten hohe Kräfte auf die Rotorenblätter, was zu Beschädigungen und erhöhtem Verschleiss führte, allerdings nicht zwangsläufig während der Angriffsphase selbst. Dies machte das Troubleshooting für die Techniker der Atomanlage zum Albtraum und erschwerte die Entdeckung von Stuxnet. Zur Tarnung zeichnete Stuxnet vor dem Angriff ausserdem 21 Sekunden lang die Werte von Sensoren der Zentrifugen auf und spielte diese Daten anschliessend in einem Loop den Überwachungssystemen im Kontrollraum zu. Als weiteren Tarnmechanismus gaben die kompromittierten Siemens-Controller falsche Auskünfte: Sollte ein Techniker während eines Angriffs Befehle an einen infizierten Controller senden, so würde er von diesem eine gefälschte Antwort erhalten, die den Normalbetrieb vortäuscht.

Nach den Manipulationen an den Zentrifugen wurde wieder in den Normalbetrieb übergegangen. Die Bereitstellung von Ersatzrotoren für die Zentrifugen war für die Techniker der Atomanlage nicht das Problem. Vielmehr waren es die ständigen Störungen der sensiblen Prozesse durch die hohe Unzuverlässigkeit der Zentrifugen, die das Anreichern von Uran verunmöglichten.

Duqu und Duqu 2.0 wurden vermutlich basierend auf dem Source Code von Stuxnet entwickelt. Ersteres infiziert Rechner durch Zero-Day-Exploits und sucht nach Informationen, die für den Angriff auf ICS-(SCADA/DCS-)Systeme relevant sein könnten. Die zweite Variante wurde unter anderem auf Rechnern in der Schweiz und in Österreich in Hotels und Lokalitäten, die in Verbindung mit den 5+1-Verhandlungen zum Atomabkommen mit Iran standen, entdeckt.

APT-Angriffe müssen aber nicht zwangsläufig auf staatlicher Ebene von Entwicklerteams mit unbegrenzten finanziellen Ressourcen und Zugang zu geheimdienstlichen Informationen durchgeführt werden. Ein anschauliches Beispiel dafür, dass einerseits mit wenig Ressourcen APT-Angriffe durchgeführt werden können und andererseits ganz gewöhnliche Firmen ins Visier von Angreifern geraten können, liefert ein Fall, der im Mai 2015 unter dem Namen «Operation Oil Tanker» bekannt wurde.

Nigerianische Betrüger griffen dabei gezielt Firmen aus dem Sektor maritime Öl- und Gastransporte an. Der Angriff wurde über Phishing-E-Mails mit einem Self-Extracting Archive, das als PDF-Datei getarnt wurde, ausgelöst. Die weiteren beim Angriff verwendeten Techniken zum gezielten Diebstahl von Passwörtern wurden nicht über Malware im üblichen Sinne durchgeführt, sondern durch Verkettung und Automatisierung von normalerweise legitimen Dateioperationen (u.a. Aufruf von Skripten, Umbenennen von Dateien, Zugriff auf Registrierungsschlüssel, Schreiben von Textdateien, Entpacken von Archiven). Diese Aktivitäten können durch Antivirensoftware nicht erkannt werden, da sie von normalen Benutzeraktivitäten nur schwer zu unterscheiden sind. Ziel des Angriffs auf die Firmen waren im Browser zwischengespei-



cherte Benutzerpasswörter, die automatisch extrahiert und auf einen FTP-Server kopiert wurden. Bei der Analyse der Passwortdateien auf dem FTP-Server durch eine IT-Sicherheitsfirma konnte festgestellt werden, dass rund zehn Firmen ausschliesslich aus dem Sektor maritime Öl- und Gastransporte durch diese Attacke kompromittiert wurden. Weiter konnte festgestellt werden, dass sich die gesammelten Passwörter bis August 2013 zurückdatieren liessen, was darauf schliessen lässt, dass die Angreifer über einen längeren Zeitraum unentdeckt Daten extrahiert haben. Nach aufwendiger Analyse und Recherche konnte rekonstruiert werden, warum zufällige Firmen aus einer bestimmten Branche angegriffen wurden: Mit den gestohlenen Passwörtern wurden Zertifikate und Dokumente erbeutet, die die Existenz von Öl und Kraftstoffen auf Öltankern belegen. Zu solchen Dokumenten gehören etwa Qualitätszertifikate, Herkunftszertifikate, Handelsvollmachten oder Frachtpapiere. Mit diesen gestohlenen Dokumenten wurde anschliessend Ölhändlern die angebliche Ladung verkauft, wobei ein branchenüblicher Vorschuss von bis zu 100 000 Dollar an die Betrüger überwiesen wird.

Solange der Angriff nicht entdeckt wird, befindet sich der Angreifer im Netzwerk, kann Daten mitlesen und manipulieren.

Bild: iStockPhoto

Veranstaltungshinweis
Cyber Security ist ein Schlagwort, das heutzutage immer wieder zu hören ist. Am Hacking Day 2015 am 9. September bringt Ihnen Digicomp die Thematik der «Advanced Persistent Threats» mit diversen Sessions und Hands-on-Labs näher.
www.digicomp.ch/hackingday

Advanced Persistent Threats auch für kleine Fische

Wie die beiden unterschiedlichen Beispiele von Stuxnet und «Operation Oil Tanker» zeigen, ist der Begriff APT sehr breit gefächert. Es gibt keinen typischen Angriffsmechanismus oder Angreifer und kein typisches Angriffsziel. Erfolgreiche APT-Angriffe sind komplex, sorgfältig geplant und gut vorbereitet. Sie stellen das Gegenstück zum klassischen «Bonny and Clyde»-Vorgehen dar, wo ein Angreifer einbricht, sich schnappt, was er kann, um dann möglichst rasch das Weite zu suchen.

Es wäre naiv zu glauben, dass nur Atomanlagen, politische Ziele oder Unternehmen mit Milliardenumsätzen in das Visier von Angreifern geraten können. APTs sind eine Bedrohung für alle Firmen, solange der Angreifer auf irgendeinem Weg gut Geld verdienen kann. Schliesslich hat jede Organisation, unabhängig von ihrer Grösse, schützenswerte Informationen, die sich versilbern lassen. Sei es letztlich durch Erpressung oder durch Weiterverkauf der Informationen. APTs sind keine neue Erscheinung, sondern der nächste logische Evolutionsschritt der Internetkriminalität.

«Der Angreifer sucht gezielt nach dem schwächsten Glied in der Kette»

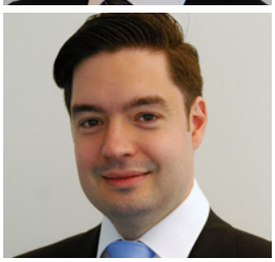
Yves Kraft und Immanuel Willi von Oneconsult, einem auf IT-Security-Beratung spezialisierten Unternehmen, erzählen im Interview unter anderem, warum sich auch KMUs vor APT-Attacken schützen müssen. Beide sind Keynote-Speaker am Hacking Day 2015. Interview: Marcel Urech

Können Sie uns in einfachen Worten erklären, was eine APT-Attacke (Advanced Persistent Threat) ist?
Yves Kraft: Ein APT ist ein komplexer, meist sorgfältig vorbereiteter Angriff, der das Ziel verfolgt, sich dauerhaften Zugriff auf das Zielobjekt, etwa ein Unternehmen oder spezifische Systeme, zu verschaffen. Solange der Angriff nicht erkannt wird, kann der Angreifer beliebige Aktivitäten wie Systemmanipulationen, digitalen Bankraub oder Datenklau betreiben.

Solche Angriffe dauern oft mehrere Monate. Wie ist es überhaupt möglich, dass sie so lange nicht erkannt werden?
Immanuel Willi: Ein Angreifer wird sich bemühen, möglichst unauffällig zu agieren. Wenn die Zugangsdaten eines Benutzers durch einen Angreifer entwendet werden können, finden alle weiteren Aktionen unter dem Kontext des Benutzers statt und sind ohne sorgfältige Analyse kaum von legitimen Benutzeraktionen zu unterscheiden. Wenn sich der Angreifer die Zeit nimmt, den Angriff sorgfältig zu planen, wird er im Vorfeld gewisse Massnahmen ergreifen, wie etwa den Einsatz von spezifisch für den Angriff programmierter oder angepasster Malware, die vom Antiviren-Scanner nicht erkannt wird. Ausserdem versuchen Angreifer, ihre Spuren zu verwischen, indem sie Logging- und Intrusion-Detection-Mechanismen aushebeln oder manipulieren.

Und welche Einfallstore nutzen Hacker für die Angriffe?
Willi: Der Angreifer sucht gezielt nach dem schwächsten Glied in der Kette, etwa ungepatchte internetzugewandte Systeme oder unvorsichtige Nutzer, die mittels Phishing angegriffen werden. Entgegen den bekannten Massenphishing-E-Mails lässt sich eine gut geschriebene und gezielt auf eine Person oder Firma entworfene Phishing-E-Mail durch den Benutzer nicht leicht als solche identifizieren. Letztlich reicht es, dass ein einzelner Benutzer den Anhang der E-Mail öffnet oder dem Link folgt und seine Zugangsdaten eingibt. Anschliessend installiert der Angreifer im Benutzerkontext des nichtsahnenden Benutzers Malware auf dem Zielsystem, damit er auch Zugriff hat, nachdem der Benutzer turnuskonform sein Passwort geändert hat.

Viele Firmen glauben, dass Virenscanner und Firewalls reichen, um sich vor Cyberattacken zu schützen. Bei APTs helfen diese Massnahmen aber nicht. Warum?
Willi: Sie helfen schon – beide sind ein elementarer Baustein der IT-Sicherheit. Da die bei vielen APT-Attacken eingesetzte Malware für den einen Angriff konzipiert wurde, wird sie von den Virenscannern nicht entdeckt, weil diese primär nach Bitmustern im Programmcode der potenziellen Malware suchen und dies bedingt, dass die Malware vom Antivirenhersteller bereits im Vorfeld untersucht werden konnte – was hier ja nicht der Fall ist. Die Firewall wird übertölpelt, indem Verbindungen mittels legitimen Benutzerdaten erfolgen.



Yves Kraft (oben) ist Team Leader Bern, Senior Penetration Tester & Security Consultant und Immanuel Willi (unten) ist Senior Security Consultant & Penetration Tester bei der Oneconsult AG. www.oneconsult.com

Beide Autoren sind Referenten am Hacking Day am 9. September 2015 in Zürch. www.digicomp.ch/hackingday

Was müssen Unternehmen zusätzlich tun, um sicher zu sein?
Kraft: Unternehmen müssen IT-Sicherheit als ganzheitliche Disziplin begreifen. Hundertprozentige Sicherheit gibt es natürlich nicht, aber Firmen können mit der Umsetzung von wenigen gezielten Massnahmen bereits viel erreichen. Deshalb braucht es ergänzende Elemente wie ein Security-Monitoring, Netzwerksegmentierungen, Benutzer-Awareness-Schulungen, ein Update-Management, die restriktive Handhabung von Benutzerrechten und viele weitere Massnahmen, die den Angreifer in der Durchführung der APT-Phasen Vorbereitung, Infektion, Verteilung und Persistenz stören. Ziel jeder Firma sollte es sein, durch mehrschichtige Abwehrmassnahmen möglichst gut gegen Angriffe geschützt zu sein. Die Strategie von «Defense in Depth» bildet ein Netz von Abwehrmassnahmen. Falls eine nicht greift, ist die Firma dennoch durch weitere Schutzmechanismen geschützt. Eine Blaupause dafür, welche Massnahmen das beste Kosten-Nutzen-Verhältnis bringen, gibt es leider nicht. Massnahmenpakete müssen bei jedem Unternehmen individuell auf dessen Kontext abgestimmt werden.

APTs zielen meist auf Grossfirmen, Branchen oder Staaten. Viele KMUs sehen sich daher nicht gefährdet. Zu Recht?
Kraft: Es gibt genügend dokumentierte Angriffe auf kleine Unternehmen. Wenn für den Angreifer der potentielle Gewinn den Aufwand übersteigt, wird er auch KMUs ins Visier nehmen. So sind oft private IT- und Pharma-Forschungsbetriebe und Family Offices per Definition KMUs – über für Dritte wertvolle Informationen verfügen sie dennoch allemal.

Was raten Sie Firmen, die nur ein kleines Budget für IT-Sicherheit haben?
Willi: Das Thema trotzdem anzugehen und ein kleines Budget nicht als Vorwand zu benutzen, um nichts zu tun. Schon mit günstigen Massnahmen wie der Sensibilisierung der Benutzer, sich an gängige Best Practices zu halten und verdächtige Vorkommnisse zu melden oder dem konsequenten Updaten von Software, kann für verhältnismässig wenig Geld viel erreicht werden. Statt blind Massnahmen zu ergreifen, sollte aber vorab eine Bedrohungsanalyse durchgeführt werden.