KOMMANDO-INTERNATIONAL SPECIAL OPERATIONS MAGAZINE

K-ISOM

www.k-isom.com

SAS
exklusiv!

NATO SPECIAL FORCES:
Belgian Special Forces Group

NATO SOF:
Komandosow, SOCSOUTH, Exercise "Flaming Star"

ÜBUNGEN UND MANÖVER:
Fused Response, Combined Resolve, Allied Spirit

ELITE:
200 Jahre Gurkhas

SCHARFSCHÜTZEN:
82nd Airborne Sniper

SEK UND JUSTIZVOLLZUG:
SFW Güstrow & Jail Special Response Team

WAFFEN:
Die HK G36-Story

Nr.5/2015 September/**Oktober**

Deutschland 6,50 €, Österreich 6,90 €
Schweiz 12,80 CHF, Belgien 7,80 €, Luxemburg 7,80 €

Bundestag muss Netzwerk aufgeben – Wieso, weshalb, warum, wer noch?

Juni, 2015: Nach Recherchen von NDR, WDR und SZ sagen Experten des Bundesamtes für Sicherheit in der Informationstechnik, das Netzwerk des Bundestags sei nach der schweren Hackerattacke die Mitte Mai 2015 entdeckt wurde nicht mehr zu retten. Es wird von einem „Totalschaden", einer „Aufgabe des Netzwerks", einem notwendigen Hardwaretausch und einer kompletten Neuinstallation gesprochen. Die Firma Corporate Trust ist nicht in diesen Fall involviert – allerdings kennt das dortige Fachpersonal die in der Presse beschriebenen Symptome aus etlichen unserer aktuellen Fälle. Daher können die Experten aus München in diesem Artikel einige Hintergrundinformationen liefern.

Voraussetzung für einen erfolgreichen Angriff ist immer die Infiltration des Zielnetzwerks. Dies wird in der Regel mit einer gezielt für das Opfer vorbereiteten, bösartigen E-Mail gemacht (sogenanntes Spear-Phishing) die dann einen Trojaner einschleust. Angesichts der Tatsache, dass der deutsche Sicherheitsapparat in der IT den Kampf gegen die Malware (Viren und Trojaner) gerade generell verliert, steigt das Risiko für jede Organisation an, Opfer einer solchen Attacke zu werden. Ist ein Trojaner einmal eingeschleust, wird versucht, an ein möglichst hochwertiges Passwort heranzukommen. Das Ziel ist typischerweise das Passwort eines IT-Administrators. Erster Schritt dazu ist es, die Kontrolle über den infizierten Rechner zu bekommen (im Fachjargon: lokale Administratorrechte). Generell gilt: je älter das System ist, desto leichter ist das. Auch die Konfiguration im Unternehmen und die Aktualität der eingespielten Updates spielt hierbei eine Rolle. Im Regelfall wird ein Angreifer in vielen Netzwerken aber sehr oft noch auf veraltete Systeme treffen (teilweise Windows XP), die ihm die Arbeit hier stark erleichtern. Oft haben in Firmen auch viele oder alle Mitarbeiter diese Rechte ohnehin – dann muss ein Angreifer hier keine weitere Zeit verschwenden.

Danach wird typischerweise eine Angriffstechnik verwendet, die sich Pass-the-Hash (PtH) nennt. Wenn ein Nutzer sich mit seinem Passwort unter Windows anmeldet, dann wird eine nicht wiederherstellbare Form dieses Passwort zwischengespeichert (diese Form nennt man Hash). Dieser Hash wird benutzt, um im Hintergrund die Anmeldung an weitere Computer weiterzureichen, damit der Benutzer das Passwort nicht ständig neu eingeben muss. Besitzt ein Angreifer lokale Administratorrechte, kann er diese Hashes verwenden um sich an weiteren Systemen anzumelden und sich dort weitere Hashes zu holen. Dies wiederholt der Angreifer solange, bis er die Berechtigung eines hohen IT-Administrators erlangen konnte. Eine solche PtH-Attacke ist eine spezielle Form des Logindaten-Diebstahls, und sie lässt sich nicht verhindern (menschliche Schwäche) – d. h. Ziel ist es, dem Angreifer das Erlangen der Voraussetzung für diese Attacke (die Administratorberechtigung) möglichst schwer zu machen (Mitarbeiterschulung bzw. Sensibilisierung).

Alle Windows PCs sind in einem Microsoft Netzwerk zusammengefasst, das sich Domäne nennt und durch mehrere spezielle Rechner (sogenannte Domain Controller) verwaltet wird. Innerhalb der Domäne werden alle Benutzerberechtigungen mit einem Kerberos genannten System verwaltet. Wenn ein Benutzer eine Anwendung im Netzwerk nutzen will, so holt er sich beim Domain Controller ein sogenanntes Kerberosticket, welches er dann bei der Anwendung die er nutzen will vorzeigt. Dieser Prozess läuft im Hintergrund in jeder Firma der Welt tausendfach ab. Auch der Leser hat sich heute sicherlich schon ein Kerberosticket besorgt. Ein Kerberosticket hat typischerweise eine Laufzeit von einigen wenigen Stunden (je nach Konfiguration zwei bis zwölf Stunden), danach ist eine Neuausstellung bzw. eine Neuanmeldung notwendig.

Ziel des Angreifers ist nun die Berechtigung eines sogenannten Domänen-Administrators. Mit dieser Berechtigung kann sich ein Angreifer dann mit einem Hackertool namens mimikatz ein sogenanntes „Golden Ticket" erstellen. Ein solches Ticket nutzen z. B. auch die Domain Controller um sich gegenseitig die vollen Berechtigungen für eine lange Laufzeit (zehn Jahre) zu geben. Stellen Sie sich vor, Sie hätten einen Schlüssel für jedes Haus und jede Wohnung in Ihrer Stadt. Und das tollste ist, wenn Sie diesen Schlüssel benutzen, dann verwandeln Sie sich gleichzeitig automatisch in den Hausbesitzer. Ein Angreifer der ein Golden Ticket besitzt, hat etwa analoge Fähigkeiten in Ihrem Netzwerk.

Der nächste Schritt des Angreifers ist nun einfach: ausgestattet mit den höchstmöglichen Berechtigungen geht es nun darum, geheime Zugangspunkte an möglichst vielen Stellen im Netzwerk zu verstecken. Das können SmartTVs in Besprechungsräumen, PCs in Robotersteuerungen, der Vorstands-PC, der Hauptrouter im Netzwerk, das Voice-over-IP Telefon des Entwicklungsleiters und jegliche andere Computertechnologie sein. Um die Sache ein bisschen komplizierter zu machen, kann sich ein Angreifer auch so tief in Hardware eingraben, dass eine Bereinigung durch eine Softwareneuinstallation nicht mehr in einem sinnvollen Kostenrahmen möglich ist und die Hardware ausgetauscht werden muss. Ein bekannter Vorfall ist z. B. die Schadsoftware der „Equation Group" die unter anderem die Fähigkeit besitzt, die Festplatten-Firmware verschiedener Hersteller darunter Seagate, Western Digital, Toshiba, Maxtor und IBM umzuschreiben. Es gibt aber bereits Hinweise, dass diese Angriffsmöglichkeit auch für die Software der Computerhauptplatine (das BIOS) bzw. für Netzwerkkarten denkbar ist.

Hat ein Angreifer erstmal ein Golden Ticket erhalten und konnte mit diesem ein paar Stunden „spielen gehen", dann ist die Aussage, dass das Netzwerk verloren ist, nicht übertrieben. Allein um das Golden Ticken zu widerrufen ist eine komplexe Nachsicherungoperation notwendig. Um aber alle Folgen einer solchen Infektion sicher zu beseitigen müssen wohl alle Rechner neuinstalliert und ggf. auch die komplette Hardware ausgetauscht werden. Dies ist nicht möglich wenn der Hacker zeitgleich noch an anderen Stellen im Netzwerk ist, d. h. für die Bereinigung muss entweder das gesamte Netz vom Internet getrennt oder alle Computer abgeschaltet werden. Dies ist normalerweise nicht möglich ohne die Existenz einer Firma zu gefährden. Im Bundestag besteht durch die Sommerpause im August eventuell sogar eine realistische Chance für eine solche Nachsicherung. Im Normalfall wird eine Firma ein so kompromittiertes Netz als „unsicheres Intranet" weiterbetreiben und mit einer neuen sicheren Keimzelle beginnend ein neues „Netzwerk im Netzwerk" aufbauen. Zuerst werden in diesem neuen Netzwerk nur die sensibelsten Daten verarbeitet später übernimmt es sukzessive die Aufgaben des alten Netzwerks. Dieser Prozess kann sich über mehrere Jahre ziehen, während derer man sich mit den Hackern im alten, unsicheren Netzwerk ein Rückzugsgefecht liefert um ihnen den weiteren Datenabfluss wenigstens so schwer wie möglich zu machen.

Lessons Learned der Corporate Trust aus sieben Jahren Abwehr von Industriespionage: Bei der derzeitigen Angriffslage müssen die Domain Controller und Domain Admins in höchstem Maße abgesichert werden. Dies bedeutet unter anderen:

- Einsatz von Application Whitelisting (z. B. Microsoft Applocker) auf den Domain Controllern,
- Einsatz einer Host Based Firewall auf den Domain Controllern,
- Intensives Logging auf den Domain Controllern,
- Reduktion der Personen mit Domain Admin Berechtigungen auf zwei, maximal drei Accounts,
- Trennung der Domain Admin Accounts von den normalen Admin Accounts,
- Verwaltung der Domain Controllern nur per RDP over IPSEC von dedizierten, hochgesicherten Bastion Hosts,
- Aufstufen des Domain Feature Level auf mindestens 2007, Nutzung aller Sicherheitsfunktionen,
- Strikte Einhaltung der Microsoft Empfehlung bzgl. Domänensicherheit,
- Konzentration auf ein verteidigbares Netzwerk. Dies bedeutet unter anderem:
- Homogenisierung der verwendeten IT-Komponenten, konsequentes abschalten veralteter Hardware bzw. Software.
- Erweiterung des heute meist dreistufigen Netzwerks (Internet - DMZ - Intranet) auf mindestens 6.8 Sicherheitszonen.
- Entwicklung einer Log Policy und überprüfen ob die Logeinstellungen an allen Servern und Clients stimmen.
- Verwendung von Einmalpasswörter für administrative Aktionen oder mittels tokenbasierter Authentifizierung.
- 100 % Sicherheit gibt es nicht. Jede Firma muss sich auf einen Angriff vorbereiten.
- Generell gilt: solange das Ausmaß des Angriffs noch nicht bekannt ist, sind Abwehrmaßnahmen reine Glückssache und selten sinnvoll und zielgerichtet einsetzbar.
- Rein technische Gegenmaßnahmen helfen in der Detektion, reduzieren Schaden und minimieren Angriffsmöglichkeiten - verhindern aber keine Industriespionage und beenden keinen laufenden Angriff. Einem gezielt vorgetragenen Angriff muss man ein mit gutem Know-How ausgestattetes Verteidigungsteam entgegenstellen, welches die technischen Sicherheitsmaßnahmen ergänzt/flankiert.
- Die Angreifer wählen die Waffen, Zeitpunkt und Schlachtfeld: d. h. sie haben freie Wahl mit welchen Tools sie wann welchen Server angreifen und haben damit einen Vorteil gegenüber der Verteidigung. Die Vorteile des Verteidigungsteams sind die bessere Kenntnis der Infrastruktur und die weitreichenderen Handlungsmöglichkeiten in der internen IT. Dazu benötigt das Verteidigungsteam ausreichende Kompetenzen damit das Team auch wirklich bessere Handlungsmöglichkeiten als die Angreifer hat.

Über Corporate Trust, Business Risk & Crisis Management GmbH: Corporate Trust ist der strategische Partner namhafter Unternehmen im Risiko- und Krisenmanagement. Als Unternehmensberatung für Sicherheitsdienstleistungen unterstützt Corporate Trust Unternehmen, Organisationen und Privatpersonen im High-Level-Security-Bereich. Sicherheitskonzepte sollten so effektiv und diskret sein, dass ihre Existenz am besten gar nicht wahrgenommen wird. Genau das ist die Mission. Corporate Trust will eine Umgebung schaffen, in der man sich absolut sicher und ungestört auf die eigenen Ziele und die Ziele des Unternehmens konzentrieren kann. Im Mittelpunkt steht dabei immer der Mensch.

Ansprechpartner:
Dipl. Inf. Florian Oelmaier
Leiter IT-Sicherheit und Computerkriminalität
CORPORATE TRUST
Business Risk & Crisis Management GmbH
Graf-zu-Castell-Str. 1
D-81829 München
Tel.: +49 89 599 88 75 80
Fax: +49 89 599 88 75 820
muhr@corporate-trust.de
www.corporate-trust.de