infonews.ch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Erfahrungen aus 15 Jahren Audits

Seit 15 Jahren bietet die GO OUT Production GmbH produkteneutrale IT-Security Audits, Penetration Tests und Beratungen für eine Vielzahl von verschiedenen Unternehmen und öffentlichen Verwaltungen an. Zeit, einmal zurück zu blicken und einige Erfahrungen und Eindrücke aufzuzeigen.

Dieser INFONEWS 1/14 geht unter anderem auf folgende Themen ein:

- Externe Sicht (Penetration Test)
- Technische Umgebung (Quick Audit)
- Organisatorische Sicht

Inhaltsverzeichnis

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Einleitung

1999 gründeten drei ZHAW-Studenten (damals noch TWI, danach ZHW) die Firma GO OUT Production GmbH. Das Ziel war es, im Bereich der IT-Sicherheit entsprechende Überprüfungen durchzuführen und passende, pragmatische Lösungen vorzuschlagen. Von Beginn weg war es aber das Ziel, keine Umsetzungen anzubieten, damit die Unabhängigkeit nicht gefährdet wird. Diesem Motto ist das inzwischen auf 10 Personen gewachsene Team treu geblieben. Dieser spezielle INFONEWS geht auf die 15 Jahre ein und zeigt einige Episoden und Vorschläge.

Dass das organisierte Verbrechen den Weg ins Internet gefunden hat, ist keine Überraschung. Bereits vor einigen Jahren hat McAfee darauf hingewiesen, dass sehr viel Geld mit Online-Kriminalität umgesetzt wird. Fast täglich kann in den Zeitungen und Fachmedien von Angriffen auf Firmen und Staaten gelesen werden. Bei unseren Vorstellungsgesprächen hören wir aber oft, dass die Firma entweder kein potentielles Ziel eines Angriffes ist oder gar keine schützenswerten Daten vorhanden sind. Unsere Erfahrung zeigt aber, dass dies klar nicht der Fall ist. Wenn eine Schwachstelle vorhanden ist, wird diese früher oder später auch gefunden und entsprechend ausgenutzt. Wir sind auch der festen Überzeugung, dass jede Firma Daten hat, die es zu schützen gilt. Die Schweiz gilt als sehr innovatives Land und hält weltweit immer noch die meisten Patente. Auch Symantec hat in ihrem Jahresbericht 2013 aufgezeigt, dass immer mehr kleine Firmen ins Visier der Angreifer kommen. Der Grund ist klar, grosse Firmen haben in der Regel Budget und Know-how entsprechende Gegenmassnahmen zu planen und umzusetzen, kleinere Firmen hingegen setzen oft nur das Nötigste ein: „Wir haben ja ein Antivirenprogramm und eine Firewall“. Dies ist zwar ein erster guter Schritt, genügt aber alleine noch nicht.

2 Angriffsziel Mensch

Der Mensch ist, egal welche Studie man liest, das Ziel Nummer 1. Es wird versucht, die Gutgläubigkeit oder die Hilfsbereitschaft schamlos auszunutzen. Ein Angriffsmittel ist Phishing. Dabei werden E-Mails mit mehr oder weniger plausiblem Inhalt zugestellt, mit der Bitte, etwas anzuklicken, zu öffnen oder einen Fragebogen auszufüllen. Für diverse Kunden durften wir bereits solche Angriffe durchführen. Dabei geht dies von plumpen DHL-E-Mails bis zu firmengerecht gestalteten E-Mails und der entsprechenden Webseite. Das E-Mail wird in der Regel im Namen einer wichtigen Person in der Firma verschickt. Die Ziel-E-Mail-Adressen erhalten wir entweder direkt vom Kunden oder suchen uns diese via Xing, Linkedin, Google und natürlich der Firmenhomepage zusammen. Obwohl das Thema Phishing schon oft behandelt wurde, haben unsere Angriffe jeweils eine zwischen 50 und 80% liegende Erfolgsquote. Es ist davon auszugehen, dass in Zukunft diese Art der Angriffe immer besser werden, dass nicht mehr holpriges Deutsch von einer Übersetzungsmaschine verwendet wird (im Stil von „Du gehen Webseite, du geben Passwort ein“), sondern gutes, zielgerichtetes Deutsch.

3 Externe Sicht

Neben dem Faktor Mensch ist der Schutz gegenüber dem Internet essentiell wichtig. Es sind so viele (Skriptkiddie) Tools frei verfügbar, die das ganze Internet nach Schwachstellen absuchen. Werden diese gefunden, werden sie auch gleich ausgenutzt. Ein Selbstversuch zeigte, dass ein ungepatchtes Windows-System nach 10 Minuten bereits

nicht mehr selber kontrolliert wird, sondern bereits von einer anderen Person übernommen wurde. Hier hilft sicherlich die bereits erwähnte Firewall. Diese muss aber stetig gepflegt werden, Regeln sind bei Nichtverwendung wieder zu löschen und vor allem ist jede Änderung zu protokollieren. Ein kurzes Konzept mit dem Umgang mit dem wichtigsten Element gegenüber dem „bösen" Internet ist essentiell. Wichtig bei der Firewall ist, dass alles geschlossen wird, was nicht wirklich benötigt wird. Any-Regeln sind dabei ein Tabu und dürfen nur mit Bedacht verwendet werden (z.B. E-Mail-Versand oder Internetseitenaufrufe nach Any, jedoch wird die Quelle (Source) dann eingeschränkt, im Falle von E-Mail darf nur der E-Mailserver E-Mails verschicken, im Falle von Internet, nur die Clients, auf keinen Fall die Server).

Vergessen beim Thema Firewall wird der Umstand, dass bewusst ein Port auf ein System geöffnet wird und damit die Firewall keinen Schutz mehr bietet (abgesehen von den UTM-Firewalls, doch leidet die Performance sehr stark, wenn jedes Paket bis ins letzte Bit untersucht wird und daher wird dieser Schutz oft wieder ausgeschaltet). Die Anfragen werden dann direkt auf das entsprechende Ziel-System weitergeleitet (FTP, E-Mail-Server, Web-Server, VPN-Endpunkt, etc.). Diese Systeme sind dann den Angriffen ausgesetzt. Ein gutes und regelmässiges Patch-Management ist dabei unentbehrlich. Wir empfehlen allerspätestens nach zwei Wochen nach der Veröffentlichung eines Patches, diesen eingespielt zu haben. Diese Pause ist zwar bereits sehr lange, verhindert aber das Einspielen eines fehlerhaften Patches.

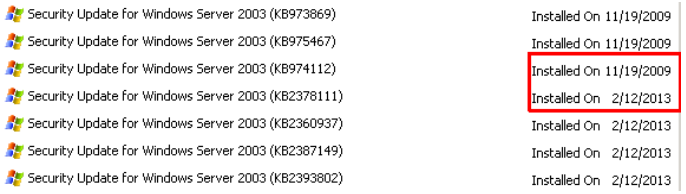

Abb. 1: Patch-Rhythmus

Aber nicht nur dem Internet ausgesetzten Systeme müssen regelmässig aktualisiert werden, sondern auch alle anderen Server UND Clients. Dies kann heute mehrheitlich automatisch erfolgen, zum Beispiel unter Windows mit dem WSUS (Windows System Update Service), jedoch gehen die vielen zusätzlichen Software-Pakete, die nicht von Microsoft kommen, vergessen. Unsere Erfahrung zeigt, dass die Hacker genau dies ausnutzen und vermehrt auf Dritt-Applikationen zugreifen, da reicht es, ein verseuchtes PDF oder eine verseuchte Flash-Datei zu öffnen und der Rechner ist infiziert. Daher müssen alle Dritt-Applikationen im Patch-Management mitberücksichtigt werden.

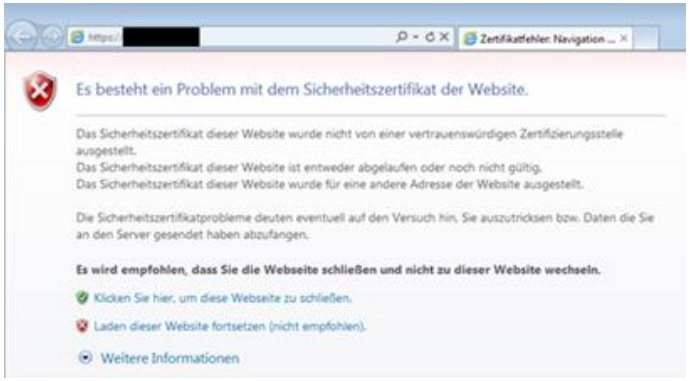

Abb. 2: Zertifikats-Fehlermeldung

Ein weiteres von uns oft festgestelltes Problem sind selber signierte Zertifikate. Dabei wird im Browser des Aufrufers

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

infonews.ch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

ein Fehler angezeigt, dass etwas mit dem Zertifikat nicht in Ordnung ist. Den Mitarbeitern wird dann mitgeteilt, dass diese Fehlermeldung korrekt sei und einfach auf „Weiter" geklickt werden soll. Wird diese Fehlermeldung dann auch beim Online-Banking (oder sonst wo) angezeigt, weiss der Mitarbeiter ja, dass dies korrekt ist. Ein fataler Irrtum!

Weiter kann auch ein Profi nicht mehr unterscheiden, ob die Verbindung korrekt aufgebaut wurde oder ob gerade ein Man-in-the-middle Angriff stattfindet (dabei hängt sich ein Hacker in die verschlüsselte Verbindung ein. Da das Zertifikat bis heute nicht so gefälscht werden kann, ohne dass es zu einem Fehler kommt, kann ein solcher Angriff entdeckt werden). Daher empfehlen wir immer öffentlich signierte Zertifikate zu verwenden.

4 Interne Sicht

Bei den internen Audits starten wir immer mit einem Rundgang. Dazu gehört die Besichtigung des Serverraumes. Wie ist der Zutritt geregelt? Welche Überwachungen und Alarmierungen erfolgen? Wie sieht die Ordnung im Raum selber aus? Wird dieser noch als Lager „missbraucht"? Gerade auf die Verkabelung muss Acht gegeben werden. Diese sollte sauber ausgeführt werden, dass schnell ersichtlich ist, wo welches Kabel hinführt.

Eine Beschriftung und verschiedene Kabelfarben sind sicherlich sinnvoll. Auch die Stromkabel sollten unterschieden werden, was geht an die USV, was nicht. Wasserleitungen sollten, falls immer möglich, nicht durch den Serverraum führen. Weiter gehört ein passender Feuerlöscher in die Nähe des Serverraumes. So können Kleinstbrände frühzeitig gelöscht werden.

Abb. 3: Ordnung im Rack

Im Bereich der Server sind sicherlich das Active Directory und der Datei-Server die wichtigsten Elemente. Beim AD ist darauf zu achten, eine eigene OU-Struktur aufzubauen. Gerade Objekte in der Standard-OU „Computers" sind schnell an den richtigen Ort zu verschieben. Auf die OU „Computers" greifen keine Gruppenrichtlinien (mit Ausnahme der Default Domain Policy). Bei der Passwort-Policy empfehlen wir mindestens 10 Zeichen inkl. Komplexität, dafür muss es nicht monatlich gewechselt werden. Im Internet sind so genannte Rainbow-Tables mit bis zu neun Zeichen umfassenden Passwörter bereits weit fortgeschritten. Mit diesen Tabellen ist ein Passwortknacken in kurzer Zeit möglich. Für wenige Dollars kann dieses Knacken auch in die Cloud verlagert werden. Auf dem Datei-Server sind

Freigaben und Berechtigungen sauber zu vergeben. Lohnenswert ist es dabei, sich an das A G DL P Prinzip von Microsoft zu halten. Der grosse Vorteil mit der Arbeit von Gruppen ist der Wechsel von Mitarbeitern, einfach austragen, neue Person eintragen, fertig. Ansonsten kann es geschehen, dass SID-Leichen übrig bleiben.

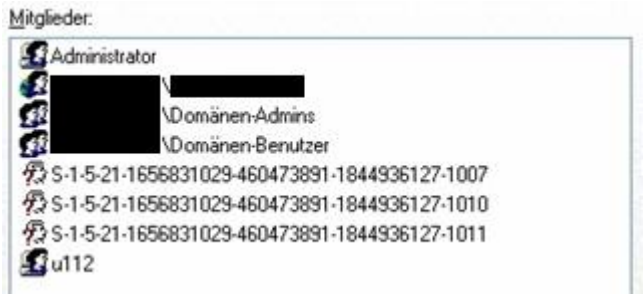

Abb. 4: SID-Leichen

Zu vermeiden ist die Vergabe von „Vollzugriff“. Damit können alle eingetragenen Benutzer und Gruppen selber weitere Rechte vergeben. Weiter zu vermeiden sind standardmässige lokale Administratorenrechte. Nicht einmal die Netzwerk- und Serverbetreuer dürfen ständig mit diesen Rechten arbeiten. Geht es wirklich nicht ohne, muss ein zweiter Account mit den benötigten Rechten erstellt werden. Nur für Aufgaben, die diese hohen Rechte benötigen, sollte dieder Benutzer verwendet werden.

Bei unseren Audits finden wir regelmässig Dateien, die nicht für alle Benutzer bestimmt sind: dies können Lizenzdaten, Passwortlisten oder dergleichen sein, die mit etwas Browsen im Firmen-Netzwerk gefunden werden können.
Die Verwendung von mobilen Geräten nimmt immer mehr zu. Firmen erlauben den Mitarbeitern die Nutzung von E-Mail und Kalender auf ihren Smartphones. Dabei werden verbindliche Vorgaben an diese Geräte vergessen. So sollte das Endgerät zwingend verschlüsselt werden. Auch ein Passwort gehört zwingend dazu, befinden sich doch oft auch sensible E-Mails plötzlich auf diesen Geräten. Auch sollte mit den Benutzern geklärt werden, was bei einem Verlust des (privaten) Gerätes geschieht. Ein Remote-Wipe löscht dabei nicht nur die Firmendaten, sondern alle (und eventuell den Cloud-Speicher gleich mit).

5 Schlusswort

Dies sind nur einige Eindrücke aus unseren vielen Audits, die wir für unsere Kundinnen und Kunden durchführen durften. Vielen Dank für das uns entgegengebrachte Vertrauen in den vergangenen 15 Jahren. Wir freuen uns, Sie auch in Zukunft mit unserem Wissen und unserer Erfahrung unterstützen zu dürfen.

Falls Sie uns noch nicht kennen, lernen Sie uns doch durch das Quick Audit kennen. Wir zeigen Ihnen, wie es um Ihre IT-Sicherheit steht und wie Sie Ihre IT-Sicherheit pragmatisch erhöhen können.

Besuchen Sie uns unter www.goSecurity.ch.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21