12 Schnelltests für die Cyber-Security

Die Widerstandsfähigkeit eines Unternehmens gegen Cyberangriffe zu testen, ist nicht so leicht wie ein Corona-Schnelltest. Leider ist es auch mit einem Penetrationstest allein nicht getan, da dieser hauptsächlich proaktive technische Schutzmaßnahmen prüft. Unser Autor liefert daher ein Dutzend (überwiegend Schnelltest-)Szenarien, um auch die eigenen Detektions- und Reaktionsfähigkeiten im Selbsttest prüfen zu können.

Von Falko Weiß, München

Bei der Prüfung eigener Sicherheitsmechanismen richtet sich der Blick von IT-Personal (und auch Penetrations-Testern) vorrangig auf die Funktion proaktiver Sicherheitselemente wie Firewalls, Anti-Malware-Systeme sowie auf Softwareupdates. Notwendige Mindeststandards zum präventiven Schutz digitaler Unternehmens-Infrastrukturen sind zwar mittlerweile öffentlich verfügbar und weithin bekannt (vgl. [1]). Befragt das Management die eigene IT zur Lage der Informations-Sicherheit, werden aber oft nur die notwendigen technischen Investitionen in diesem Bereich betrachtet und es kommt nicht selten zu einer Überschätzung der eigenen Abwehrfähigkeiten. Doch defensive technische Schutzmaßnahmen allein genügen längst nicht mehr!

Bei der heutigen Professionalität im Cybercrime muss man davon ausgehen, dass Angreifer sämtliche defensive Schutzmaßnahmen überwinden können – beziehungsweise schon überwunden haben. Um dann nicht die Waffen strecken zu müssen, sind im Sinne von „Assume the Breach" weitere Elemente wesentlicher Teil einer Cybersicherheitsstrategie:

- Erkennung von Sicherheitsvorfällen
- technische Reaktionsmöglichkeit auf Cyberangriffe
- Krisenreaktion bei einem Cybersicherheitsvorfall

Und genauso wie defensive Schutzmaßnahmen durch Penetrationstests zu überprüfen sind, müssen auch diese drei Elemente getestet werden. Egal, ob entsprechende Leistungen von internen Abteilungen oder externen Dienstleistern erbracht werden: Ohne regelmäßige Tests und Übungen ist die Effektivität im Ernstfall nicht gewährleistet!

Richtig Testen

Schlüsselpunkt einer erfolgreichen Teststrategie ist die regelmäßige Durchführung – ein jährlicher Turnus hat sich dabei bewährt. Den Testkatalog sollte man im gleichen Rhythmus überarbeiten: Echtfälle aus der praktischen Arbeit aufnehmen, weniger relevante Tests nur noch alle zwei, drei oder fünf Jahre durchführen. Im Folgenden sind als Startpunkt für den eigenen Testkatalog der ersten Iteration 12 Tests aufgeführt.

Die Durchführung dieser Tests kann relativ rasch hintereinander (z. B. ein Test pro Tag) oder sogar parallelisiert im Rahmen einer mehrtätigen Übung stattfinden. Denkbar ist aber auch ein Testzeitraum von ein bis drei Monaten. Wichtig ist ein definierter Test-Abschluss, um im gemeinsamen „Lessons Learned"-Workshop den Verbesserungsprozess einleiten zu können.

Die hier vorgestellten Tests orientieren sich an Echtfällen und den aktuellen Vorgehensweisen der organisierten Kriminalität (OK). Die beigefügte Begründung ermöglicht dabei eine Priorisierung gemäß der eigenen Bedrohungsanalyse im Unternehmen. Sollten andere Täter, wie beispielsweise Geheimdienste, Innentäter oder Konkurrenten, in der Bedrohungsanalyse eine wichtige Rolle spielen, müssen die Tests entsprechend ergänzt werden.

Das Vorgehen der Schnelltests ist jeweils praxiserprobt und zumeist einfach durchführbar – nur einige Tests erfordern einen mittleren bis sehr hohen Aufwand, was bei den jeweiligen Szenarien angemerkt ist. Jeder Testinhalt ist für sich offensichtlich und muss von einer IT-Sicherheitsorganisation erfolgreich bearbeitet werden können. Die Szenarien sind nicht subtil, sondern zielen auf Ereignisse, die sich einfach erkennen lassen – das entspricht der aktuellen Vorgehensweise der organisierten Kriminalität. In Zukunft mag es aber durchaus notwendig werden, auch verstecktere Indizien zu betrachten.

Die hier vorgestellten Tests fokussieren im Rahmen eines „Assume the Breach"-Paradigmas die Erkennung, Reaktion und (Krisen-)Bearbeitung von Vorfällen. Dabei wird gegebenenfalls die Überwindung von technischen Schutzmaßnahmen (z. B. durch eine Zero-Day-Schwachstelle) angenommen. Die proaktiven technischen Schutzmaßnahmen selbst sollte man unab-

hängig hiervon überprüfen – beispielsweise durch einen Penetrationstest.

Test #1: Gerätediebstahl

Szenario: Am Freitag um 21 Uhr wird am Bahnhof der Laptop eines Mitarbeiters gestohlen, auf dem sich wichtige Daten befinden. Der Mitarbeiter meldet dies der Hotline und bittet um Hilfe.

Hintergrund: Es kommt häufig vor, dass Laptops, Mobiltelefone oder Datenträger mit wichtigen Daten verloren gehen oder gestohlen werden. Wird dies vom betroffenen Mitarbeiter gemeldet, darf das Thema nicht bis zum Montag warten, denn wichtige Firmendaten könnten in Gefahr sein oder sogar eine Meldung gemäß DSGVO notwendig werden.

Testvorgehen: Melden Sie einen Firmenlaptop an der Hotline am Freitag um 21:00 Uhr als gestohlen. Verfolgen Sie den Prozess als Benutzer und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab: Maßnahmen wie eine Prüfung, ob das Gerät verschlüsselt und zugriffsgeschützt war, eine Ortung, eine Sperrung von Zugängen, die auf dem Gerät gespeichert sein können, und die Fernlöschung des Gerätes sind sinnvoll. Der Fall sollte innerhalb von 3 Stunden bearbeitet sein. Für die schnelle Zuweisung eines Ersatzgeräts gibt es Bonuspunkte.

Test #2: Phishing

Szenario: Ein Mitarbeiter meldet sich, weil eine E-Mail mit einem Link angekommen ist. Er hat auf den Link geklickt, um ein Dokument herunterzuladen und musste seine Office365-Kennung (oder andere Benutzerdaten) und den zweiten Faktor eintippen. Der Mitarbeiter berichtet, dass das Dokument eine Falle war – es gab nur eine Fehlermeldung. Er glaubt, er hat einen Fehler gemacht und bittet um Hilfe.

Hintergrund: Phishing-E-Mails sind einer der häufigsten Angriffe, um Zugangsdaten zu erlangen, gegebenenfalls Daten zu stehlen oder weiter in ein Unternehmen vorzustoßen.

Testvorgehen: Nutzen Sie eine vorhandene Phishing-E-Mail oder schicken Sie von einer neutralen, externen E-Mail-Adresse eine Phishing-Mail mit einem Link an den Mitarbeiter – die Domain muss existieren, die einzelne Seite darf einen Fehler melden. Häufig sind solche Links nur einmalig aufrufbar. Melden Sie den Vorfall an der Hotline. Verfolgen Sie den Prozess als Benutzer und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab: Eine gute Reaktion beginnt mit der sofortigen Deaktivierung des Benutzerkontos für den Zeitraum der Analyse. Eine Prüfung der E-Mail, die Prüfung von Sicherheitsprotokollen auf Aktivitäten nach Verlust des Zugangs, eine Bereinigung betroffener Systeme sowie die Änderung des Passworts führen zu einem guten Ergebnis.

Test #3: Passwortangriff

Szenario: Auf einer externen Schnittstelle (z. B. Internetportal) erfolgt ein Angriff mit dem Ziel, über das Erraten/Durchprobieren von Passwörtern einen Zugang zur Unternehmensinfrastruktur zu erlangen. Ziele können beispielsweise Terminalserver, Outlook Web Access (OWA) oder ein VPN-Zugang sein. Nach einigen Versuchen kommt es zu einem erfolgreichen Login.

Hintergrund: Der Angriff auf Benutzerkonten mit schwachen oder gestohlenen Passwörtern führt häufig zu einem erfolgreichen Eindringen in Unternehmen. Ein Angreifer kann auf diese Art Fuß fassen, Daten stehlen und sich weiter ausbreiten.

Testvorgehen: Um einen Passwortangriff zu simulieren, braucht man Grundkenntnisse über Angriffswerkzeuge (z. B. „Hydra") sowie Vorgehensweisen von

Bruteforce-, Password-Spray- oder Credential-Stuffing-Angriffen – Wissen über die interne IT wird jedoch nicht benötigt. Testen Sie mit einem externen Client und einer Liste falscher Passwörter, an deren Ende der valide Login zum gewählten Benutzerkonto steht. Verfolgen Sie den Prozess als Beobachter und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab: Der erfolgreiche „Angriff" sollte spätestens am nächsten Tag erkannt werden. Eine Vorgehensweise analog zum Phishing – also die Deaktivierung des Benutzerkontos, die Sicherung und Prüfung von Logs auf Aktivitäten nach dem Login, eine Bereinigung und Änderung des Passworts – führt zu einem guten Ergebnis.

Test #4: Payment-Diversion

Szenario (mittlerer Aufwand!): Im Einkauf trifft eine E-Mail von einem Lieferanten ein, welche auf eine echte E-Mail antwortet, die ein Mitarbeiter vor einer Weile geschrieben hat. Inhalt: Die Kontonummer des Lieferanten hätte sich durch Umstrukturierung geändert, Rechnungen sollen in Zukunft bitte an die enthaltene neue Kontonummer gezahlt werden.

Hintergrund: Payment-Diversion ist ein häufiger Angriff auf die Buchhaltung eines Unternehmens. Durch die Umleitung regelmäßiger Zahlungen an ein vom Angreifer kontrolliertes Konto können hohe Summen verloren gehen.

Testvorgehen: Zur Vorbereitung wird eine echte Konversation mit dem Lieferanten benötigt. Durch eine gefälschte E-Mail, die an die echte Konversation anschließt, wird dem Mitarbeiter oder der Abteilung die neue Bankverbindung mitgeteilt. Die E-Mail trägt im From-Header die E-Mail-Adresse des Lieferanten oder eine, die sehr ähnlich aussieht – diese wurde jedoch gefälscht, kostenfreie Dienste gibt es dazu im Internet. Verfolgen Sie den Prozess als Beobachter und intervenieren Sie, wenn die Kontoverbindung geändert wird. Prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab: Der Angriff sollte durch bestehende Prozesse wie einen Rückruf bei Kontoänderungen sofort auffallen. Die Erkennung und Vermeidung der Kontoänderung führen zu einem guten Ergebnis.

Test #5: Scannen nach Zugängen

Szenario: Von einem unkritischen System aus wird die Netzwerkinfrastruktur gescannt. Der Scan umfasst wichtige Schnittstellen für die Weiterbewegung eines Angreifers – RDP, VNC, SMB, SSH, RPC und weitere. Der Scan erfolgt aus einem Benutzerkonto ohne Domain-Admin-Rechte – der Mitarbeiter selbst ist dabei nicht aktiv.

Hintergrund: Nachdem ein Angreifer sich Zugang zu einem Unternehmen verschafft hat, versucht er sich zu orientieren, schlecht gesicherte Zugänge zu erkennen und sich zu einem System vorzuarbeiten, wo er seine Rechte erhöhen kann (Privilege Escalation).

Testvorgehen: Von einem Mitarbeiter-Client werden unter Windows ein nmap, Advanced IP Scanner oder eine ähnliche Software ausgeführt und die IP-Ranges möglichst breit gescannt. Verfolgen Sie den Prozess als Benutzer und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab: Die Durchführung des Scans sollte einen Alarm auslösen und der Sicherheitsorganisation auffallen. Der Alarm muss spätestens am nächsten Tag bearbeitet werden. Die Erkennung, die Überprüfung des Quellsystems, eine Deaktivierung des Benutzerkontos und die Einrichtung einer Sicherheitsüberwachung zur Prüfung auf weitere Anomalien führen zu einem guten Ergebnis.

Test #6: Schadsoftware

Szenario: Auf ein unternehmenskritisches System wird über das Netzwerk ein Angriffswerkzeug aufgebracht und ausgeführt, zum Beispiel die Software Bloodhound oder Mimikatz auf einem Domaincontroller.

Hintergrund: Domaincontroller sind das zentrale Nervensystem einer Unternehmensinfrastruktur und daher primäres Ziel eines Ransomware-Angreifers. Es besteht die Gefahr, dass Angreifer hier privilegierte Zugänge stehlen – im schlimmsten Fall mutieren sie zum Domain-Administrator.

Testvorgehen: Vor dem Test sollte der IT-Leiter eingeweiht werden, um Panik zu vermeiden. Ein Benutzerkonto, möglichst ohne Domain-Admin-Rechte, wird eingesetzt (z. B. ein Backup-User oder das Benutzerkonto eines Mitarbeiters). Die Software Bloodhound oder Mimikatz wird nachts direkt vom System aus dem Internet heruntergeladen oder auf das System kopiert und ausgeführt. Wird dies vom Anti-Malware-System verhindert, stört das den Test nicht. Verfolgen Sie den Prozess und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab: Die eingesetzte Software oder der Anti-Malware-Alarm müssen sofort erkannt und der Vorfall bearbeitet werden. Logs müssen gesichert und ausgewertet werden, um festzustellen, wie die Angriffswerkzeuge auf das System kamen und wozu sie genutzt wurden. Die schnelle Durchführung, das Erkennen der Bedrohung und das Einberufen eines Krisenstabes oder

eines Teams zur Abstimmung von Maßnahmen sind ein gutes Ergebnis.

Test #7: Datendiebstahl

Szenario: Von einem (File-)Server – notfalls von einem Client aus – werden mit dem Benutzerkonto des Domänen-Administrators über Nacht 10 Gigabyte Daten auf einen Server im Internet hochgeladen.

Hintergrund: Der Diebstahl einer größeren Menge von Daten ist bei einem Verschlüsselungsangriff mit Ransomware mittlerweile die Regel. Mit der Veröffentlichung der Daten soll das Unternehmen zusätzlich erpresst werden. Auch im Bereich der Wirtschaftsspionage spielt Datendiebstahl naturgemäß eine große Rolle.

Testvorgehen: Mit einem Administrator-Account der Domäne (idealerweise Domain-Admin) werden vom ausgesuchten Server 10 GB Daten an ein Ziel in der Cloud hochgeladen. Dies sollte ein kontrollierter eigener Server, Dropbox-Account oder etwas Ähnliches sein. Verfolgen Sie den Prozess und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab: Moderne Sicherheitssysteme sollten Anomalien dieser Art erfassen und Alarm geben – der Einsatz eines (Domain-)Administrator-Kontos ist ein zusätzliches und absolut kritisches Warnsignal. Die Sicherheitsorganisation sollte den Vorfall spätestens am Folgetag erkennen, bestehende Logs sichern und prüfen sowie einen schwerwiegenden Sicherheitsvorfall melden. Werden der Einsatz des Administratoraccounts und die Notlage erkannt, ist dies ein gutes Ergebnis.

Test #8: Backups löschen

Szenario: Mit dem Benutzerkonto des Domänen- oder Backup-Administrators wird ein Backup gelöscht.

Hintergrund: Die Löschung von Backups durch den Domänen-Administrator oder mit dem Backup-User ist Standard bei einem Ransomwareangriff. Auf diese Weise soll die Wiederherstellung verschlüsselter Daten und Systeme aus dem Backup unmöglich gemacht werden.

Testvorgehen: Hier muss man ein wenig von der Realität eines Echtangriffs abweichen! Anstatt Backup-Daten tatsächlich zu löschen, sollte das gesamte Backup mit den Rechten des Backup- oder Domänen-Adminstrators um 22 Uhr abends einmalig deaktiviert werden. Verfolgen Sie den Prozess und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab: Die Deaktivierung (d. h. die simulierte Löschung) des Backups muss sofort erkannt werden. Weniger als eine sofortige Einberufung eines Krisenmeetings und eine Abstimmung weiterer Maßnahmen sind an dieser Stelle ungenügend! Der Zusammenhang mit einem Angriff muss erkannt werden. Könnte ein Angreifer das Backup mit den höchsten Rechten aller Benutzerkonten der Infrastruktur nicht löschen, gibt es jedoch Bonuspunkte.

Test #9: DDoS-Angriff

Szenario: Der Internetanschluss oder die Website des Unternehmens wird durch Distributed-Denial-of-Service (DDoS) angegriffen. Parallel dazu erhält das Unternehmen eine Erpressernotiz über öffentlich bekannte E-Mail-Adressen. Der Täter verlangt eine Summe in Bitcoin, ansonsten werde das Unternehmen sechs Tage später mit voller Kraft und dauerhaft angegriffen.

Hintergrund: DDoS-Erpressungen kommen häufig vor und können jedes Unternehmen treffen. Der Angriff kann ein Unternehmen vom Internet trennen und wichtige Plattformen unerreichbar machen.

Testvorgehen (mittlerer Aufwand!): Der Test sollte mit dem IT-Leiter und unter Umständen externen Partnern/Anbietern abgestimmt werden, um einen Aufschrei