Pentesting und Co. – Sicherheitstests auf verschiedenen Levels

Infolge des zunehmenden Drucks durch Angriffe professioneller Ransomwaregruppen steigt für Firmen und öffentliche Einrichtungen die Notwendigkeit, die eigene Organisation resilienter zu machen. Ein Weg dahin führt über Pentesting und technische Prüfungen wie Red Teaming.

Von Hagen Molzer

Angesichts der sich häufenden gezielten Angriffe durch kompetente und motivierte Angreifergruppen, auch APTs (Advanced Persistent Threats) genannt, müssen Unternehmen reagieren. Um ihre Geschäftsabläufe zu schützen, müssen sie ihre Risiken und Schwachstellen kennen und Maßnahmen zur Behebung oder Reduzierung des Risikos ergreifen. Bewährte Mittel dafür sind die vielfältigen technischen Prüfungsarten wie Schwachstellenscans, Pentesting oder Red Teaming. Welche kommen für verschiedene Organisationen, abhängig von ihrem Reifegrad, infrage?

Die Reihenfolge der nachfolgend beschriebenen Varianten technischer Sicherheitsprüfungen orientiert sich an ihrer Komplexität sowie dem nötigen Reifegrad der Organisation in Bezug auf die implementierten Sicherheitsmaßnahmen und gegebenenfalls vorbereitend durchgeführte Prüfungen. Die zuerst beschriebenen Prüfarten sind also grundlegend und weniger komplex, während die zuletzt genannten nur für große Finanzdienstleister sinnvoll sind, die verschiedene Regularien erfüllen müssen und deren IT-Security-Maßnahmen bereits einen sehr hohen Reifegrad aufweisen.

Netzwerk- und Schwachstellenscans

Die einfachste Form der Überprüfung besteht aus Netzwerk- und Schwachstellenscans. Mit einem gängigen Schwachstellenscanner prüft man damit regelmäßig die eigene Infrastruktur auf Lücken. Diese Scanner finden beispielsweise veraltete und schwachstellenbehaftete Software- und Betriebssystemversionen oder offensichtliche Lücken in deren Konfiguration.

Dies ist die grundlegendste Form eines Sicherheitstests, die jede Organisation regelmäßig durchführen sollte. Dabei sollte zunächst die aus dem Internet erreichbare Infrastruktur geprüft werden, da diese Systeme am exponiertesten sind. Im nächsten Schritt folgt dann das interne Netzwerk.

Die Scans erfordern vergleichsweise wenig Aufwand, auch externe Dienstleister können sie durchführen. Diese übernehmen auch die Aufbereitung der Scanergebnisse und verifizieren, ob es sich bei den Befunden um False Positives handelt oder ob tatsächlich Handlungsbedarf besteht.

Die eigentliche Arbeit beginnt jedoch erst nach diesen Sicherheitsscans und umfasst zum Beispiel:

- das Priorisieren von Maßnahmen unter Hinzuziehen der jeweiligen Systemverantwortlichen,
- das Planen und Aufspielen von Updates für die veralteten Betriebssystem- und Softwareversionen sowie
- das Planen und Durchführen von Konfigurationsanpassungen zur Behebung der Schwachstellen.

Als Ergebnis erhält man eine sehr breite, aber oberflächliche Übersicht zu Schwachstellen in der IT-Infrastruktur auf Dienstebene. Auf weniger offensichtliche Schwachstellen, beispielsweise in spezifischen Webanwendungen oder in über das Netzwerk erreichbaren Diensten, wird nicht geprüft. Bezüglich des Reifegrades erfordert diese Sicherheitsüberprüfung keine Voraussetzungen.

Penetrationstests spezifischer Anwendungen und Dienste

Hierbei konzentriert sich der Penetrationstester auf eine oder wenige Webanwendungen oder konkrete Dienste und sucht, größtenteils manuell, nach Schwachstellen in den Prüfobjekten. Findet er welche, versucht er sie auszunutzen, gegebenenfalls nach Rücksprache mit dem beauftragenden Unternehmen, um das von der Schwachstelle ausgehende Risiko zu belegen.

Ziel ist hier, auf effiziente Weise möglichst viele Schwachstellen zu finden. Typischerweise stellt das Unternehmen Zugangsdaten bereit, damit die Tester mit wenig Aufwand auch Schwachstellen finden, die hinter einer Benutzeranmeldung liegen. Auch hier sollte die Organisation zunächst mit dem Überprüfen öffentlich erreichbarer Webanwendungen und Dienste beginnen.

Das Resultat besteht aus einem klassischen Penetrationstestbericht mit den gefundenen technischen Schwachstellen und Empfehlungen zur Behebung. Die Dokumentation einer Schwachstelle umfasst eine detaillierte Beschreibung des Sachstands, Informationen zur Ausnutzung sowie eine Einschätzung der Kritikalität und potenziellen Auswirkungen einer Ausnutzung. Auch diese Sicherheitsüberprüfung erfordert bezüglich des Reifegrades keine Voraussetzungen.

Innentäteranalyse: Assumed-Breach-Penetrationstest

Bei dieser Prüfart simuliert der Tester, dass ein Angreifer bereits Zugriff auf das interne Netzwerk hat und über Zugangsdaten eines regulären Benutzers verfügt. Davon ausgehend untersucht er das interne Netzwerk auf Schwachstellen. Dabei versucht er typischerweise ein oder mehrere mit der Organisation abgestimmte Ziele zu erreichen, etwa die vollständige Kompromittierung der Active-Directory-Domäne. Die Domäneninfrastruktur ist somit häufig eines der Hauptziele für Lateral-Movement- und Privilege-Escalation-Angriffe.

Die übergeordnete Aufgabe des Penetrationstesters ist es, möglichst viele Schwachstellen zu finden, auszunutzen und gegebenenfalls zu verketten, um am Ende eines solchen Angriffspfads das oder die vereinbarten Ziele zu erreichen. Im klassischen Durchführungsmodus weiß das Administrationsteam des Kunden über die Tests Bescheid, sodass es potenziell ausgelöste Alarme ignoriert und keine Gegenmaßnahmen ergreift.

Der Penetrationstester kann somit effizient vorgehen, da die Angriffe nicht unentdeckt bleiben müssen. Dadurch findet er potenziell mehr Schwachstellen in kürzerer Zeit.

Im Stealthy-Modus ist das anders. Hier soll der Penetrationstester die vereinbarten Ziele unerkannt erreichen, dazu muss er vorsichtiger und langsamer vorgehen. Das bedeutet oft, dass er weniger Schwachstellen findet oder für das Projekt mehr Zeit veranschlagen muss. Der Vorteil für den Kunden ist aber, dass er gleichzeitig seine Maßnahmen zur Angriffserkennung und Alarmierung testet. Das kann interessante Ergebnisse liefern, insbesondere wenn Angriffserkennung und Reaktion an externe Dienstleister wie Managed Security Service Provider ausgelagert wurden. Sollte der Penetrationstester „auffliegen", wird in den klassischen Modus gewechselt, um effizient nach weiteren Schwachstellen zu suchen.

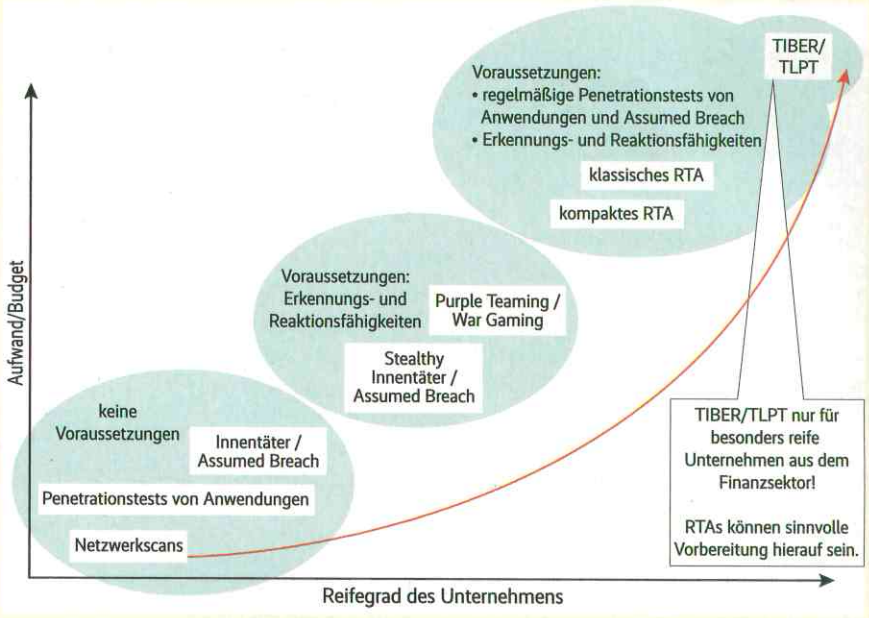
Häufig führt man diese Überprüfung auch „Stealthy to Loud" durch, also mit dem Ziel, spätestens am Ende der Überprüfung auf jeden Fall einen Alarm auszulösen. Das gibt der Organisation einerseits eine grobe Orientierung darin, wo sich die Alarmschwelle befindet, und anderseits kann die Reaktion auf Alarme durch die Verteidiger zuverlässig beobachtet werden.

Am Ende steht ein klassischer Penetrationstestbericht mit den technischen und konzeptionellen Befunden, denn häufig kann man aus den gefundenen Schwachstellen auch auf konzeptionelle Schwachstellen schließen – einschließlich Empfehlungen zur Behebung. Falls gewünscht, kann der Tester eine detaillierte Liste der durchgeführten Angriffe erstellen. Damit kann der Kunde im Nachgang nach Spuren der Angriffe in Logdateien und Produkten zur Angriffserkennung suchen.

Anforderungen an den Reifegrad für den klassischen Modus der Überprüfung gibt es keine. Für den Stealthy- oder Stealthy-to-Loud-Modus sollten aber Maßnahmen zur Angriffserkennung und Reaktion implementiert sein, beispielsweise ein EDR- oder XDR-System (Endpoint Detection and Response, Extended Detection and Response), ein SIEM (Security Information and Event Management) oder es muss ein MSSP-Dienstleister angebunden und beauftragt sein.

Lernen mit War Gaming

Beim War Gaming geht es nicht darum, technische Schwachstellen aufzudecken,



Die verschiedenen Prüfungsarten erfordern unterschiedliche Voraussetzungen und damit Reifegrade in einem Unternehmen. Zu den herausforderndsten Sicherheitstests gehören das Red-Team-Assessment (RTA) und seine Weiterentwicklung, das Threat-led Penetration Testing (TLPT).

sondern darum, das Blue Team (siehe unten) zu trainieren. Dabei wird ein reales Angriffsszenario simuliert. Um so eine Angriffskette vollständig durchlaufen zu können, kann es sogar sinnvoll sein, temporär bestimmte realitätsnahe Schwachstellen speziell für dieses Szenario zu schaffen. Somit kann das Blue Team die Reaktion auf einen Sicherheitsvorfall unter „realen" Bedingungen in der eigenen Umgebung trainieren.

Bei dieser Art Sicherheitstests sind verschiedene Teams beteiligt, deren Rolle mit einer Farbe assoziiert wird:

- Das Red Team sind die Angreifer (beispielsweise die Penetrationstester eines externen Dienstleisters).
- Das Blue Team sind die Verteidiger.
- Das White Team sind die Personen, die auf Unternehmensseite in die Projektdurchführung eingeweiht sind.
- Beim Purple Teaming interagieren Mitglieder des roten und des blauen Teams und simulieren reale Angriffe.

Zunächst planen die Angreifer zusammen mit dem White Team ein Angriffsszenario, das am Tag der Durchführung des Projekts in der produktiven Umgebung des Kundenunternehmens abgespielt wird. Ein simples Beispiel: Ein Mitarbeiter erhält eine Phishingmail mit der Aufforderung, eine Schadsoftware auszuführen. Ein in die Übung eingeweihter Mitarbeiter simuliert das Opfer und befolgt die Anweisungen. So erhält der Angreifer Zugriff auf das interne Netzwerk und beginnt mit den im Vorfeld mit dem White Team abgestimmten Lateral-Movement-Angriffen. Dabei löst er absichtlich Alarme aus und bewegt sich weiter im Netzwerk, um am Ende auf einem speziell für die Übung installierten Server eine Demo-Ransomware auszuführen.

Learning by Doing

Zusätzlich ist ein weiterer Penetrationstester involviert, der das Blue Team vor Ort beobachtet. Er befindet sich im selben Raum, kennt das Angriffsszenario, macht sich Notizen zur Vorfallsbearbeitung, gibt aber keine Tipps. Das Blue Team weiß zwar von der Durchführung der Übung, hat aber keine Informationen über den Inhalt des Szenarios. Daraus leitet sich übrigens auch der Name Purple Teaming ab, denn die Mischung der Farben Red und Blue ergibt Purple.

Der Beobachter achtet beispielsweise

- auf Abläufe und Aufgabenverteilung im Blue Team;
- darauf, wie die Vorfallsbehandlung dokumentiert wird;
- darauf, ob eventuell festgelegte Abläufe eingehalten und Playbooks befolgt werden;
- auf die Effizienz der Analyse;
- auf die Kommunikation mit anderen Bereichen der Organisation.

Zum Tagesabschluss findet eine Besprechung mit dem Angreifer, den Verteidigern und dem Beobachter statt, in der der Ablauf der Übung besprochen wird. Das wertvollste Ergebnis der Durchführung eines solchen Projekts sind die Erfahrungen, die das Blue Team im Rahmen der Bearbeitung sammelt. Ergänzt

wird das durch die Erkenntnisse des Beobachters, die in einem Abschlussdokument zusammengefasst werden. Er hält auch fest, wo noch Verbesserungspotenzial besteht, etwa in der teaminternen Organisation und Kommunikation unter Stress, der Verwendung technischer Werkzeuge, der Dokumentation der Vorfallsbehandlung, beim Vorgehen bei der technischen Analyse oder im Beheben blinder Flecken in der Angriffserkennung.

Zur Durchführung eines Purple Teaming sollte eine Organisation bereits die oben genannten Maßnahmen zur Angriffserkennung (EDR/XDR et cetera) umgesetzt oder einen MSSP eingebunden haben. Außerdem sollten grundlegende Prozesse und Verantwortlichkeiten zur Vorfallsbearbeitung definiert und implementiert sein. Es ist sinnvoll, diese Übung regelmäßig zu wiederholen (ein- oder zweimal im Jahr), um das Gelernte zu festigen und die Schwierigkeit der Szenarien steigern zu können.

Red Teaming

Red Teaming bezeichnet eine ganzheitliche Simulation eines Angriffs durch einen motivierten und kompetenten Angreifer. Dabei simuliert das Red Team verschiedene TTPs (Tactics, Techniques and Procedures) entlang der typischen Phasen eines Angriffs nach dem MITRE ATT&CK Framework: Reconnaissance, Initial Access, Lateral Movement, Privilege Escalation, Persistence, Exfiltration und Impact.

Beteiligt sind das Red, das Blue und das White Team, wobei das Blue Team in diesem Fall nicht eingeweiht ist. So werden die Reaktionsfähigkeit und die Prozesse unter möglichst realen Bedingungen geprüft.

Um den initialen Zugriff auf das interne Netzwerk zu bekommen, führt das Red Team häufig auf Social Engineering basierende Angriffe wie Phishing oder Vishing (Phishing per Sprachanruf) durch oder es versucht, in ein Gebäude der Organisation zu gelangen. Anschließend sucht es nach technischen Schwachstellen im internen Netzwerk und nutzt sie aus. Dabei versucht das Red Team, unter dem Radar der Erkennungstechnik und des Blue Teams zu bleiben. Der Zweck: die vom Kunden vorgegebenen Ziele unerkannt zu erreichen. Im besten Fall ergibt sich im Rahmen des Projekts ein Katz-und-Maus-Spiel, wobei das Blue Team an verschiedenen Stellen auf den Angriff aufmerksam wird, Gegenmaßnahmen ergreift und so seine Reaktionsfähigkeiten trainiert.

Fliegender Wechsel

Falls das Red Team seine Ziele zügig und unerkannt erreicht, kann in Rücksprache mit dem White Team in den War-Gaming-Modus gewechselt werden, in dem dann nach weiteren Schwachstellen gesucht, jetzt aber absichtlich auffälliger vorgegangen wird. Typischerweise erstreckt sich ein Red-Team-Assessment über einen längeren Zeitraum, etwa mehrere Monate, sodass das Red Team flexibel auf verschiedene Eventualitäten reagieren kann.

Das Abschlussdokument enthält neben einem klassischen Penetrationstestbericht mit den technischen Schwachstellen auch die gewonnenen Erkenntnisse des Red Teams über Verbesserungspotenziale bei Incident-Response-Maßnahmen, blinde Flecken in der Angriffserkennung und Details zu den durchgeführten Angriffen. So können die Verteidiger im Nachgang prüfen, wie es zu den blinden Flecken kommen konnte. Im Rahmen eines ausführlichen Blue-Team-Workshops besprechen die Angreifer und Verteidiger am Ende eines Projekts noch einmal detailliert das Vorgehen, die Maßnahmen und die jeweiligen Lessons Learned.

Eine Übung für Unternehmen mit höherem Reifegrad

Bei einem Red-Team-Assessment sind ähnliche Voraussetzungen erforderlich wie beim War Gaming. Zusätzlich sollten im Vorfeld mindestens ein, eventuell aber auch schon mehrere Assumed-Breach-Penetrationstests durchgeführt worden sein, in deren Folge offensichtliche Schwachstellen behoben wurden.

Red-Team-Assessments und War Gaming können sich auch sehr gut ergänzen. Während beim War Gaming der Schwerpunkt vor allem auf das Training des Blue Teams gelegt wird, erfolgt beim Red Teaming durch den ganzheitlichen Ansatz mit sehr offenem Umfang zusätzlich eine Suche nach technischen Schwachstellen. Es ist im Vergleich das aufwendigere Projekt.

Um den Aufwand merklich zu reduzieren, ohne die Prüftiefe und -breite zu beeinträchtigen, kann das Red Teaming auch in kompakter Form durchgeführt werden. In diesem Fall verzichtet das Red Team auf eine umfangreiche Informationsgewinnungsphase; stattdessen stellt das White Team die erforderlichen Informationen bereit, etwa Mitarbeiterlisten, Informationen zur Firmenstruktur oder Bilder von Mitarbeiterausweisen.

Soll der Aufwand noch weiter reduziert oder über einen längeren Zeitraum gestreckt werden, kann man das Assessment auch in zwei Teile aufteilen. Der erste Teil ist ein „Initial-Access-Penetrationstest" mit dem Ziel, den initialen Zugriff auf das interne Netzwerk und Zugangsdaten von regulären Benutzern zu erhalten. Zu einem späteren Zeitpunkt können im zweiten Teil dann die gewonnenen Resultate dazu dienen, mit einem Stealthy-Assumed-Breach-Penetrationstest weiterzumachen.

Red Teaming für die Finanzbranche

Für regulierte Organisationen der Finanzbranche sind zwei weitere Red-Teaming-Varianten relevant: zum einen nach dem EU-Framework TIBER (Threat Intelligence-based Ethical Red Teaming), zum andern das TLPT (Threat-led Penetration Testing) nach DORA (Digital Operational Resilience Act).

Vorgehen, Ziele und Ergebnis decken sich mit denen eines Red Teaming, jedoch betten sie sich in ein größeres Framework ein und sind aufwendiger. So wird hier ein größeres Augenmerk auf die Vorgehensweisen (TTPs) von Angreifergruppen gelegt, bei denen die Wahrscheinlichkeit höher ist, dass die Organisation tatsächlich ins Fadenkreuz dieser Gruppen gerät. Außerdem wird das Projekt zum Beispiel von der Deutschen Bundesbank begleitet, die am Ende eine Durchführungsbestätigung ausstellt.

Perspektivisch ist davon auszugehen, dass die BaFin künftig mehr und mehr Finanzinstitute dazu verpflichten wird, TLPTs durchzuführen und alle drei Jahre zu wiederholen. Es kann also sinnvoll sein, sich mit „kleineren" Überprüfungen wie regulären Red Teamings oder War Gaming darauf vorzubereiten, noch bevor die Aufsichtsbehörden zuschauen. (ur@ix.de)

HAGEN MOLZER

ist Leitender Berater bei der cirosec GmbH. In seinen Schwerpunktbereichen Active-Directory-Sicherheit und Social Engineering führt er Red-Team-Assessments, Penetrationstests und Beratungsprojekte durch.