Sicherheits-Schwachstellen entdecken als Dienstleistung

Mehr Cybersecurity durch Penetrationstests

Ein Penetrationstest eröffnet Unternehmen, Instituten und Behörden die Chance, unbekannte Schwachstellen zu erkennen, bevor ein Angreifer sie ausnutzen kann. Was können solche beauftragten Hackerangriffs-Simulationen leisten?

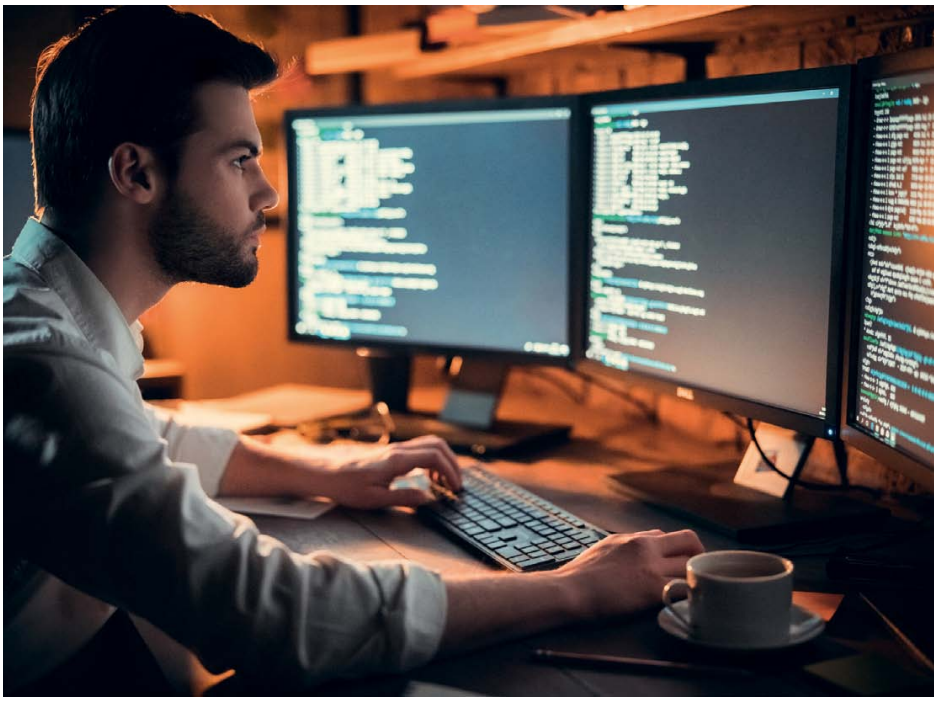
Von Severin Quell, Director IT Security Consulting bei Infodas, und Aaron Brown, dort Team Leader Security Audit

Das Angriffsziel war prominent, der Einsatz ambitioniert: Im Sommer 2020 gelang es der Ben-Gurion-Universität im israelischen Be'er Scheva, aktuelle Fahrerassistenzsysteme von Tesla zu manipulieren. Sie kaperten Werbetafeln am Straßenrand und spielten entlangfahrenden Tesla-Fahrzeugen für nur 0,42 Sekunden ein Stoppschild vor. Die Autos bremsten aus voller Fahrt. Während die Werbetafeln vermutlich mit klassischen Methoden gehackt wurden, geschah die Manipulation der Kameras und der KI-basierten Auswertungssysteme der Fahrzeuge über neue Kanäle. Damit hatten die Studenten einen der ersten erfolgreichen „Social Engineering"-Angriffe auf eine KI realisiert.

Im Oktober 2020 etwa wurde bekannt, dass „Forscher" auf den Websites von Apple in nur drei Monaten 55 zum Teil schwerwiegende Fehler gefunden hatten. Einer der schlimmsten hätte es Cyberkriminellen ermöglicht, einen Wurm einzuschleusen, der automatisch alle Fotos, Videos und Dokumente aus dem iCloud-Konto einer Person mitsamt den Kontaktdaten hätte stehlen können. Die nicht beauftragten „Forscher" meldeten die Fehler an Apple und erhielten dafür insgesamt fast 289.000 Dollar.

Anfang November deckte ein Computersicherheits-Experte auf dem Webserver der CSU-Landtagsfraktion unaufgefordert mehrere schwere Sicherheitslücken auf und verschaffte sich so unter anderem Zugriff auf die Zugangsdaten von mehr als 800 CSU-Politikern, Mitarbeitern und anderen Nutzern. Die Sicherheitslücken sind inzwischen geschlossen.

Drei Fälle, unterschiedliche Motive und Ausgangslagen, aber immer ein Ziel: Sicherheitsmaßnahmen zu überwinden und sich als unbefugter Dritter Zugang zu digitalen Assets zu verschaffen. Diese Beispiele und die aktuellen Zahlen aus dem aktuellen BSI-Report illustrieren, wie rasch die Verwundbarkeit von Wirtschaft und Gesellschaft durch Cyber-Attacken wächst. Seit Covid-19 sind zudem verstärkt Forschungsgruppen, Impfstoffentwickler und Einrichtungen des Gesundheitssystems im Fadenkreuz.



Ein Penetrationstest ist in vielen Fällen die einzige Möglichkeit, in der Unternehmens- und Behörden-IT unbekannte Schwachstellen zu erkennen, bevor ein Angreifer sie ausnutzen kann.

Schwachstellen vor den Angreifern erkennen

Umso erstaunlicher ist, dass ein Viertel aller IT-Sicherheitsfachleute nicht weiß, was ein Penetrationstest ist. Dies ist zumindest das Ergebnis einer aktuellen Umfrage des Marktforschungsinstituts Civey im Auftrag von TÜV Rheinland aus dem Sommer 2020. Das Ergebnis lässt aufhorchen, denn ein Penetrationstest ist in vielen Fällen die einzige Möglichkeit, in der Unternehmens- und Behörden-IT unbekannte Schwachstellen zu erkennen, bevor ein Angreifer sie ausnutzen kann.

Angesichts der technischen Aufrüstung auf Angreiferseite, unter anderem durch künstliche Intelligenz (siehe Kasten), wird es für Unternehmen und Öffentliche Hand immer wichtiger, Cyberkriminellen nicht nur technisch, sondern auch in puncto Manpower möglichst einen Schritt voraus zu sein. Eins der wichtigsten Tools aus dem Werkzeugkasten der Cybersecurity-Experten ist der Penetrationstest, auch Ethical Hacking genannt. Penetrationstests sind in vielen Fällen die einzige Möglichkeit, Schwachstellen rechtzeitig und vor Angreifern zu erkennen.

Fälschlicherweise wird der Begriff des Penetrationstests häufig synonym mit Sicherheitsanalyse oder Schwachstellenanalyse verwendet, deshalb hier eine Begriffsklärung: Bei der Sicherheitsanalyse gehen Cybersecurity-Spezialisten von der Dokumentenlage und Netzwerkarchitektur aus und verschaffen sich einen Überblick über den betrachteten Informationsverbund und seine Sicherheitsmaßnahmen. Hier können ergänzend technische Prüfungen zum Einsatz kommen.

Die Schwachstellenanalyse umfasst eine konkrete Untersuchung auf bekannte Schwachstellen. Dazu werden auch Tools eingesetzt. Diese decken bekannte Sicherheitslücken relativ schnell auf. Die Schwachstellenanalyse ist techniklastig, standardisiert und fördert erfahrungsgemäß zeitnah Ergebnisse zutage. Das Detektieren neuer oder komplexer Schwachstellen ist mit der Schwachstellenanalyse nicht möglich.

Der Penetrationstest ist ein beauftragter, autorisierter, geplanter und simulierter Cyber-Angriff auf alles, was mit dem Auftraggeber vereinbart wird: also etwa das Netzwerk mit einigen oder allen angeschlossenen Anwendungen, Netzdiensten und ausgewählten oder sämtlichen Datenbanken. Penetrationstester denken wie Cyberkriminelle, verfügen über exklusives Wissen der Hacker-Szene und nutzen Scan Tools und Datenbanken, um sich durch Infrastrukturen, Systeme und Anwendungen durchzuackern. Sie durchstöbern Schnittstellen, um bisher selbst vom Hersteller nicht entdeckte Schlupflöcher auszunutzen, hebeln systematisch Sicherheitsmaßnahmen aus und dringen so weit wie möglich und in der vereinbarten Angriffstiefe in ein Sicherheitssystem vor. Damit ist der Penetrationstest ein ideales Instrument, um die Resilienz von Sicherungssystemen offenzulegen. Er ermöglicht eine Risikobewertung über die aktuelle Sicherheitslage eines IT-Systems und dessen Infrastruktur und lässt Schlüsse darüber zu, inwieweit sich unbefugte Externe oder auch interne Mitarbeiter Zugang zu vertraulichen Informationen beschaffen können.

Drei Angriffsmethoden bei Penetrationstests

Für die Durchführung eines Penetrationstests benötigt ein IT-Sicherheitsanalytiker den ausdrücklichen Auftrag des Kunden und abgestimmte Informationen. Erhält er keine weiteren Informationen, handelt es sich um einen sogenannten Black-Box-Test. Bei einem White-Box-Test bekommt der Dienstleister grundlegende Informationen über das System, das er penetrieren soll, sowie – idealerweise – auch das IT-Sicherheitskonzept mit der Dokumentation der zugehörigen IT-Infrastruktur. Wird nur ein gewisser Teil der möglichen Informationen vorab zur Verfügung gestellt, wird oft auch von einem Grey-Box-Test gesprochen.

Weil die Penetrationstester das Vorgehen einer Gruppe von Angreifern simulieren, werden sie oft auch als „Red Team" bezeichnet. Ist nicht nur die Antwort der Schutzmechanismen und Sicherheitsmaßnahmen im Fokus des Tests, sondern steht auch die Schnelligkeit und Kompetenz der Sicherheitsexperten des Auftraggebers auf dem Prüfstein, nennt man diese korrespondierend oft „Blue Team".

Im Rahmen von Penetrationstests können drei Angriffsmethoden zum Einsatz kommen: ein Angriff über das Netzwerk, Social Engineering oder der physische Angriff. Nicht jede Methode ist überall sinnvoll, ethisch vertretbar oder vom Auftraggeber erwünscht. Der derzeit am häufigsten beauftragten Penetrationstest ist der Angriff über das Netzwerk. Meist gliedert sich ein Penetrationstest grob in fünf Phasen:

1. Vorbereitung (Abstimmung von Testzielen, Fokus, Prüfmethoden- und Geräten)

2. Informationsbeschaffung (Dokumentensichtung, Google-Hacking, Netzwerk-Mitschnitt, Portscans)

3. Analyse und Angriffsauswahl (Recherche nach geeigneten Exploits, detaillierte Netzwerkanalyse, Hash Cracking, Abstimmung weiterer Angriffe)

4. Verifikationstests (Ausnutzung der Schwachstellen, Umgehung von Sicherheits-

Wettrüsten zwischen Angreifern und Verteidigern

Die nächste Runde beginnt

Unter anderem durch den verstärkten Einsatz von Künstlicher Intelligenz werden Cyber-Attacken immer komplexer, mögliche Auswirkungen noch potenziert. Auch Hacker gehen gern den komfortablen Weg. Komplexe Algorithmen werden nicht mehr aufwändig von Menschen konzipiert und programmiert, sondern durch KI. Das schließt mit ein, dass auch die KI selbst Ziel eines Angriffs wird. Wird das berüchtigte Machine Learning Poisoning auf KI-Sicherheitssysteme angewendet, werden die vom Algorithmus verwendeten Trainingsdaten für Sicherheitssysteme schon bei der Software-Entwicklung „vergiftet". Das Ziel: die Trainingsdaten so zu manipulieren, dass sich unbemerkt eingebaute Backdoors zu einem späteren Zeitpunkt nutzen lassen, um Schad-Code in das abgesicherte Netzwerk einzuschleusen, mit dem Datenspionage oder Ransomware-Attacken durchgeführt werden können.

Weil damit zu rechnen ist, dass der Einsatz von KI auf Seiten der Cyber-Kriminellen noch zunimmt, wird die KI-Kompetenz von Penetrationstestern immer wichtiger. Dazu gehört unter anderem die Fähigkeit, eigene KI-Systeme mit geeigneten Trainingsdaten anzulernen, oder die Identifikation und Verringerung von False Positives, also das zuverlässige Aussortieren von falsch-positiven Warnungen sowie das Management der KI durch menschliche Intelligenz. (ak)

maßnahmen und aktives Eindringen, Man-in-the-Middle-Attacks, Post-Exploitation)

5. Abschlussanalyse (Auswertung und Dokumentation der Ergebnisse, Management Summary und Präsentation, Auflistung der Schwachstellen, Empfehlungen für Gegenmaßnahmen).

Vertrag zwischen Auftraggeber und Dienstleister unerlässlich

Wer einen Penetrationstest beauftragen will, sollte den Dienstleister seiner Wahl nach seinem Vorgehensmodell fragen. Leitfäden wie die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und das OSSTMM (Open Source Security Testing Methodology Manual) sind etablierte Standards. Zusätzlich ist zu prüfen, ob der Anbieter und sein Personal über geeignete Zertifizierungen als Sicherheitsdienstleister, etwa durch das BSI, verfügen.

Ein schriftlicher Vertrag zwischen Auftraggeber und Dienstleister ist unerlässlich. Er definiert,

- welche Aufgaben der Penetrationstester übernimmt,
- welche Risiken bei der Durchführung der vereinbarten Tests bestehen,
- in welchem Zeitraum der Test stattfinden soll,
- wie die Notfallregelung aussieht, wenn sich der Test anders als erwartet auf das System auswirkt,
- die Geheimhaltungsvereinbarung für den Auftragnehmer,
- inwieweit Rechtsabteilung und Betriebsrat in die Vorbereitung eines Penetrationstests eingebunden sind.

Menschliche Intelligenz als Gatekeeper

In Sachen Cybersecurity bleibt der Mensch der limitierende Faktor. Einerseits, weil er durch Manipulier- und Verführbarkeit selbst bei den besten Systemen die größte Schwachstelle ist, andererseits, weil der Experte Mensch immer noch die beste Koryphäe darstellt, um mit Kreativität noch unbekannte Sicherheitslücken aufzuspüren und Angreifer durch das Detektieren und Schließen von Schwachstellen in die Schranken zu weisen – auch und gerade, wenn KI mit im Spiel ist.

Alle Unternehmen sollten daher ihre IT-Sicherheitsstrategie regelmäßig überprüfen und zur Härtung ihrer Systeme nicht nur auf technische Vorkehrungen wie etwa Schwachstellen-Scanner setzen.

Allein regelmäßige und in kurzen Abständen durchgeführte Penetrationstests, aber auch der Wechsel des Penetrationstester-Teams – andere Menschen finden andere Fehler – bieten die Chance, neue Schwachstellen zu finden und die eigenen digitalen Assets zu schützen. Jede Sekunde vor dem nächsten Black-Hat Hacker zählt. (ak)

Mit Continuous Security und Shared Responsibility zum Erfolg

Sicheres Cloud Computing heute

Weil immer mehr Unternehmen auf ein immer größeres Angebot von Cloud-Lösungen zurückgreifen, kommt es in zunehmendem Maße auf geeignete Cybersecurity-Lösungen an. Welche technischen Möglichkeiten gibt es dafür, und welche Zertifizierungsverfahren sind derzeit im Entstehen?

Von Christian Banse, Abteilungsleiter des Bereichs Service und Application Security am Fraunhofer AISEC und Leiter der Geschäftsstelle des Fraunhofer Cluster of Excellence Cognitive Internet Technologies (CCIT)

Das Cloud-Computing-Angebot wächst immer weiter, so dass auch der Bedarf an Sicherheitslösungen zunimmt, die speziell auf die Bedürfnisse von Cloud- und Container-Diensten zugeschnitten sind. Denn traditionelle Sicherheitslösungen sind den Herausforderungen in der Cloud oft nicht gewachsen, weil sie statisch und nicht dynamisch bzw. kontinuierlich arbeiten. So zwingt die Dynamik der Cloud – etwa die automatische Skalierung und flexible Provisionierung von Ressourcen – Unternehmen dazu, stets einen Überblick über die Sicherheit ihrer genutzten oder angebotenen Services zu behalten, um sicher vor Angriffen oder Datenabflüssen zu sein.

Das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC beschäftigt sich schon seit einigen Jahren mit den Konzepten der „Continuous Security", also der kontinuierlichen Sicherheit, und dem Modell der „Shared Responsibility". Als Shared Responsibility versteht man die Aufteilung des Verantwortungsbereichs zwischen Cloud-Provider und Cloud-Nutzer. In mehreren Forschungsprojekten wie NGCert und EU-SEC (https://www.sec-cert.eu) forschte das Institut an Lösungen und Technologien, die die Sicherheit in der Cloud kontinuierlich überprüfen, und