unternehmer magazin

65. Jahrgang · G 4012 · 12,50 Euro

unternehmermagazin

Inhaber im Mittelstand • Zeitschrift für Familienunternehmen

3/4 • 2017

75.000 Auflage

Titelthema

Standort Deutschland

Industrie 4.0 | Daten und Datensicherheit

Special

Mittelstands-finanzierung

Titelthema
Digitale Transformation
Erfolgsstrategie von TRUMPF

Extra
D&O-Versicherung
Probleme im Schadensfall

Special
Überlegene Leistungen
FinTechs auf dem Vormarsch

Penetrationstests in der IT

Angreifbare Schwachstellen finden und schließen

Hand aufs Herz: Wann haben Sie die Sicherheit Ihrer IT zuletzt professionell geprüft? Und haben Sie Ihre Systeme dabei einem echten Stresstest unterzogen? Falls ja und wirklich erst vor kurzem, können Sie ruhig schlafen. Cyberangriffe wie im Frühjahr mit den beiden Kryptotrojanern »WannaCry« und »Petya/NotPetya«, werden Ihnen wohl auch auf lange Sicht nichts anhaben können.

Was aber, wenn Sie »Jein« sagen oder »schon eine Weile her«, auch wenn die gerade zitierte Erpresser-Schadsoftware Sie jetzt noch einmal verschont hat? Dann ist es wohl doch an der Zeit, das Thema aktiv anzugehen, am besten mit regelmäßigen Penetrationstests. Diesem Verfahren kommt in IT-Sicherheitsprüfungen aus gutem Grund wachsende Bedeutung zu. Viele Firmen unternehmen zwar mit ISO- und BSI-Zertifizierungen sowie mit Audits aller Art einiges, um ihre IT-Sicherheit zu verbessern. Doch diese Ansätze reichen offenbar nicht aus, wie die globalen Infektionen mit »WannaCry« und »Petya/NotPetya« erschreckend zeigen.

Verbreitete Maßnahmen der IT-Qualitätssicherung wie »Code-Reviews«, der »Security Development Lifecycle« oder Grundschutz- und ISO-Zertifizierungen dienen dazu, 99 % der IT-Systeme zu immunisieren. Entscheidend ist aber die Restverwundbarkeit von 1 %. Findet ein Angreifer die digitale Schwachstelle und dringt trotz der anderen Maßnahmen ins Netzwerk ein, kann er Schaden anrichten. Jede noch so winzige Sicherheitslücke reicht, um eine sonst robuste IT-Infrastruktur verletzbar zu machen. So infizierte die Schadsoftware »Petya/NotPetya« erst einzelne Systeme und pflanzte sich dann im Unternehmensnetzwerk über dieselbe Schwachstelle so wie »WannaCry« fort.

Regelmäßig Hackerangriffe simulieren ▸
Ein Penetrationstester simuliert eine Hackerattacke unter realen, aber kontrollierten Bedingungen, indem ein erfahrener IT-Spezialist in die Rolle externer Angreifer schlüpft, um Sicherheitslücken aufzudecken, bevor sie missbraucht werden können. Dabei ist zu bedenken, dass täglich irgendwo auf der Welt neue Sicherheitslücken in Softwareprodukten entdeckt werden, so dass ständig auch neue Einfallstore für Hacker entstehen. Im Fall von »WannaCry« leistete sogar der US-Geheimdienst NSA Schützenhilfe. Die NSA kannte diese Schwachstelle im Betriebssystem Windows, auf der die Weiterverbreitung des Trojaners fußte (»EternalBlue«), schon lange. Anstatt jedoch die Sicherheitslücke dem Hersteller zu melden, wurde sie als Hoheitswissen geheim gehalten, um Windows-Systeme selbst angreifen zu können.

Vor diesem Hintergrund sollten Penetrationstests in die IT-Sicherheitsprüfpläne von Unternehmen integriert und regelmäßig durchgeführt werden, um Schwachstellen proaktiv zu identifizieren und zu schließen, bevor sich Trojaner einnisten und womöglich Jahre lang unentdeckt bleiben. Penetrationstests simulieren und untersuchen ein bestimmtes Angriffsszenario oder auch mehrere, die vom jeweiligen Unternehmen vorgegeben werden. Was geschieht und wie es stattfindet, legen Auftraggeber anhand von fünf Prüfkriterien mit konkreten Bezügen auf ihre IT-Situation fest. Dabei geht es immer um die Gewinnung derselben Erkenntnisse. Danach ist man klüger.

- Ursprung eines Angriffs (Von wo?)
- Ziel eines Angriffs, der sogenannte »Scope« (Was?)
- Die Testtiefe (Wie lange?)
- Die Testmittel (Wie?)
- Die Motivation und den Wissensstand des Angreifers (Wer?)

Sebastian Schreiber

Da Penetrationstester ihr Spezialwissen permanent aktualisieren, sollten solche Untersuchungen nicht nur von der eigenen IT-Abteilung vorgenommen werden. Die Fachabteilung hat ein so breites Aufgabengebiet, das die absolute Fokussierung auf die IT-Sicherheit kaum darstellbar sein wird, und sie könnte auch bei aller Professionalität ein Stück weit betriebsblind sein. Der unbefangene Blick von außen erbringt fast immer Erkenntnisse und wertvolle Hinweise.

Penetrationstests können zeitnah erfolgen, sind preiswert und für Unternehmen nicht mit großem Aufwand verbunden. Liegt der Prüfbericht vor, zeigt sich noch ein Vorzug: Die Resultate sind sehr häufig von bestechender Klarheit. Die Befunde und ihre denkbaren Folgen lassen sich in der Regel eindeutig interpretieren und sind auch für Nicht-Informatiker zu verstehen: Weist ein Penetrationstester etwa nach, dass er in nur wenigen Stunden sämtliche Kundendaten aus der internen Datenbank auslesen kann, ist eigentlich kein Gegenargument möglich. Die IT des Unternehmens ist so gefährdet, dass sofort Schutzmaßnahmen zu treffen sind. Im Übrigen liefern Tester Abschlussberichte, die nicht nur die Lücken benennen und beschreiben, sondern auch praktische Vorschläge machen, wie man sie behebt. Die IT-Abteilung erhält ein Pflichtenheft, um die Sicherheit aller Systeme zu optimieren. Nachtests klären dann im Nachhinein, ob die Fehler behoben wurden.

Penetrationstester vergeben anders als andere Prüfer kein Siegel mit der Aufschrift »Sichere IT«, weil niemand weiß, ob nicht bald nach einem gut überstandenen Check im Internet abermals Probleme auftauchen, die gerade noch als sicher erklärte Systeme wieder angreifbar machen. Penetrationstest sollten daher turnusmäßig stattfinden. Die Kreativität der Tester besteht darin, genauso zu denken wie böswillige Hacker. Angreifer und Tester beschreiten dabei neue Wege, um Schwachstellen dort zu entdecken, wo andere Prüfinstrumente nicht suchen. ■

Sebastian Schreiber, Geschäftsführender Gesellschafter SySS GmbH, Tübingen

Trügerische Sicherheit • Lieber selbst attackieren als heimgesucht werden