Das Schweizer Industriemagazin. Seit 1972.

Mit Schnell-zugriff

maschinenbau

Nr. 7 Juli 2016

IT-Sicherheitstraining

Ohne Kenntnisse bei der IT-Sicherheit kommt heute kein Unternehmen mehr aus. Denn die zunehmende Digitalisierung sowie die rasanten Entwicklungen hin zur Industrie 4.0 und zum «Internet of things» stellen hohe Anforderungen an die Mitarbeiter. Doch wie können sie auf dem neusten Stand bleiben, ihr Wissen vertiefen und Know-how sammeln?

Der Markt für qualifizierte Weiterbildung ist überschaubar und es ist fraglich, inwieweit die bestehenden Modelle geeignet sind, das Wissen effektiv und nachhaltig in die Unternehmen zu bringen. Einen neuen, webbasierten Ansatz verfolgt die SKYTALE Online Akademie für IT-Sicherheit, die zum Angriff bläst auf eine Maschine, die voller Schwachstellen steckt.

Die Studie der BITKOM [1] aus dem Frühjahr 2015 und BITKOM-Präsident Prof. Dieter Kempf sprechen eine deutliche Sprache: Digitale Angriffe «sind eine reale Gefahr für Unternehmen. Gerade der Mittelstand muss beim Thema IT-Sicherheit nachlegen.» Untermauert wird diese Forderung durch eine Untersuchung von TÜV SÜD. Das Unternehmen hatte mit Hard- und Software ein kleines Wasserwerk einer deutschen Kleinstadt simuliert, um Hacker anzulocken [2]. Das Ergebnis dieses Honeynet-Projekts: In acht Monaten konnten über 60'000 Zugriffe aus mehr als 150 Ländern registriert werden. Auch Industrieprotokolle wurden dazu genutzt. Das beweist, dass Web-Spione, Datendiebe und Saboteure auch vernetzte Produktionsstätten und Infrastrukturen gezielt ausforschen und Angriffe vorbereiten können. Es besteht also dringender Handlungsbedarf, um die IT-Sicherheit nicht nur im Office-Bereich sondern auch in Produktionsstätten, Industrieanlagen und Infrastrukturen zu erhöhen. Doch wie kann das konkret erreicht werden? Verfügen die Entwickler, Konstrukteure und Maschinenbauer über das notwendige Know-how, um die Anlagen effektiv vor unberechtigten Zugriffen, Manipulationsversuchen und Sabotageakten zu schützen? Obwohl naheliegend, spielt das Thema Fort- und Weiterbildung in diesem Bereich bislang keine allzu grosse Rolle in Politik, Wirtschaft und den Medien.

ZUM AUTOR

Dipl.-Inf. Max Ziegler,
Akademieleiter
SKYTALE Online-Akademie für
IT-Sicherheit, Lippertor 2
D-59555 Lippstadt

Telefon +49 (0)2941 66096 90
http://skytale.academy
mz@skytale.academy

Industrieanlagen auch digital sichern

Unternehmen und ihre Spezialisten, die ihre Fähigkeiten und Kompetenzen in diesem Bereich ausbauen und vertiefen möchten, stehen nicht selten vor einer Herausforderung: Das Tagesgeschäft bindet die Ressourcen. Falls Zeit und Geld für mehrtägige Workshops und Fortbildungen vorhanden sind, fehlt es oft an Möglichkeiten, die meist theoretischen Lerninhalte schnell in der Praxis umzusetzen und dauerhaft zu festigen. Denn zurück im «business as usual» gerät das neue Wissen meist schnell wieder in Vergessenheit.

Daneben bleibt die Möglichkeit, den komplexen Lernstoff nach Feierabend über Fachbücher oder Video-Tutorials im Internet zu konsumieren. Dann bleiben jedoch nicht selten die Didaktik und auch die praktische Umsetzung des Gelernten auf der Strecke. Die Vorteile der zeitlichen und räumlichen Unabhängigkeit sowie den konkreten Bezug zur betrieblichen Praxis kombiniert die SKYTALE Online Akademie in ihrem neuen Fortbildungskurs zur Sicherheit von Web-Applikationen, die immer häufiger dazu genutzt werden, um die Produktionsprozesse im Blick zu behalten und Maschinen miteinander zu vernetzen. In fünf Kursmodulen vertiefen die Teilnehmer/innen ihr Wissen rund um die Sicherheit der Web-Apps. Innerhalb von fünf Monaten kann der Kurs berufsbegleitend absolviert und mit Zertifikat abgeschlossen werden.

Lernplattform-App.

Angriff auf eine virtuelle Maschine

Der Kurs behandelt zu Beginn die grundlegenden Fragestellungen rund um die Sicherheit von Web-Applikationen, frischt Basiswissen auf und bringt die Teilnehmer zügig auf ein hohes

fachliches Niveau. Neben den allgemeinen Grundprinzipien der IT-Sicherheit stehen zunächst systematische Risikoanalysen, Sicherheitsarchitekturen sowie die verschiedenen Netzwerktechnologien, Methoden zur Verschlüsselung, Authentifizierung und Sicherheitszertifikate im Fokus.

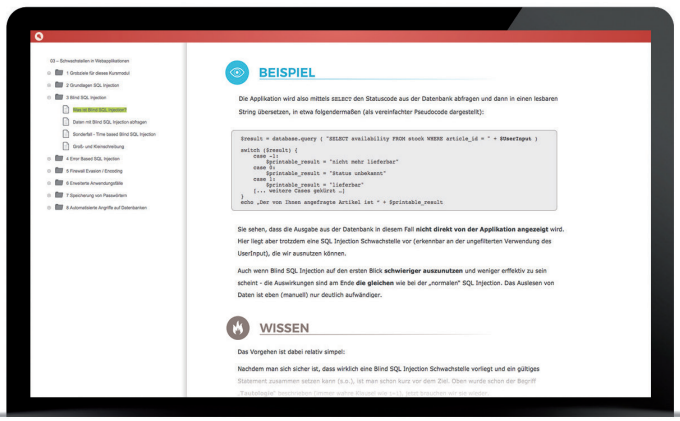
Anschliessend werden die Applikationen näher betrachtet und das Augenmerk auf potenzielle Schwachstellen, fehlerhafte Programmierung und Implementierung gerichtet. Dazu wird zunächst die Perspektive des Angreifers eingenommen, denn den roten Faden und den Kern des Lehrplans bildet eine virtuelle Maschine, die einen fiktiven Online-Shop simuliert. Dessen Web-Applikationen enthalten vielfältige Schwachstellen und Sicherheitslücken, die es im Kursverlauf zu finden gilt.

In der nächsten Phase werden durch die Aufgaben und Übungen von den Kursteilnehmern alle notwendigen Informationen über das System gesammelt und Software, Dienste und der virtuelle Webserver systematisch analysiert. Die Ergebnisse bilden wiederum die Basis für die folgenden Kursmodule, bei denen die einzelnen, konkreten Schwachstellen der Web-Applikationen näher beleuchtet werden: Die sichere Speicherung von Passwörtern, die SQL-Injection inklusive kniffeliger Spezialfälle sowie weitere Injection-Angriffe und Sicherheitslücken. Typische Fehler im Berechtigungskonzept werden dabei ebenso detailliert behandelt wie der falsche Einsatz von veralteten oder ungeeigneten Kryptographieverfahren.

Schwachstellen identifizieren und beseitigen

Ein weiterer Themenkomplex behandelt Angriffe, bei denen nicht die Web-Applikation selbst, sondern ihre Nutzer und Kunden ins Fadenkreuz der Hacker gelangen. Dazu werden beispielsweise verschiedene Varianten des Cross Site Scripting (XSS) und der Cross Site Request Forgery (CSRF) behandelt – zwei komplexe Schwachstellen, die seit Jahren in der Branche bekannt sind. Für Schlagzeilen und wirtschaftlichen Schaden sorgen sie indes auch heute noch. Sie sind häufig in den verschiedensten Web-Applikationen zu finden, obwohl sie sich im Prinzip einfach beseitigen lassen.

Deshalb werden im gesamten Kursverlauf neben den potenziellen Sicherheitslücken gleichzeitig deren Ursachen und damit mögliche Gegenmassnahmen thematisiert. Durch praktische Übungen werden sie zugleich trainiert. Der Kurs geht somit bei allen sicherheitsrelevanten Fragestellungen ins Detail: Wie gelangen Hacker über eine fehlerhafte App durch eine Firewall ins interne Firmen- und Produktionsnetz? Und wie kann das verhindert werden? Wie wird eine Anwendung effektiv auf Fehler überprüft? Wie können typische und folgenreiche Konfigurationsfehler von Web- und Applikationsservern vermieden werden? Die Antworten vermitteln die Dozenten nicht nur anhand von verständlichen Texten, Tutorials und konkreten Aufgaben. Bei Fragen können sich die Studierenden an die IT-Sicherheitsexperten wenden. Per E-Mail und Telefon geben sie individuell Feedback und helfen, wenn die Teilnehmer allein nicht weiterkommen.



Lernplattform.

Literatur
[1] https://www.bitkom.org/Presse/Presseinformation/Digitale-Angriffe-auf-jedes-zweite-Unternehmen.html
[2] http://www.tuev-sued.de/tuev-sued-konzern/presse/pressearchiv/potenzielle-angreifer-sind-ueberall

Beim Design auch Sicherheit einbauen

Damit bietet der Kurs gewissermassen eine allgemein anwendbare Anleitung zur Entwicklung von inhärent sicheren Applikationen. Das vermittelte Know-how ist essenziell von der Planung bis zum Release. Denn «Security by design» kann nur gelingen, wenn die Beteiligten entlang der gesamten Wertschöpfungskette ihren Blick für sicherheitsrelevante Aspekte schärfen, der potenziellen Risiken und Bedrohungen «aware» sind und eigenständig Lösungen für den konkreten Anwendungsfall entwickeln können.

Dies ist eine notwendige Voraussetzung für den vielfach geforderten Kulturwandel in der Software-Entwicklung, bei dem die Sicherheit der Systeme ins Zentrum rückt. Denn meist stehen auch heute noch Nutzerfreundlichkeit, Performance, Kompatibilität, Ressourcen- und Kosteneffizienz sowie Optik und Design allein im Vordergrund. Sicherheit lässt sich jedoch nur gewinnen, wenn sie von vornherein in sämtlichen Phasen berücksichtigt wird. In der Theorie ist das mittlerweile weit verbreiteter Konsens. Doch in der betrieblichen Praxis wird noch allzu häufig offenbar, dass dieses Konzept steht und fällt – mit dem Know-how der Mitarbeiter.