MEHR ZUM THEMA

OneConsult → **www.oneconsult.com**
Technische Security Audits nach OSSTMM → **www.isecom.org/press/hakin9_OSSTMM_DE.pdf**

IT-BERATERKATALOG

Das Adressbuch der Schweizer IT-Branche
→ **www.computerworld.ch/services/itberater**

Security: Testen im Team

Internationale Projekte mit mehreren Teams und verteilten IT-Hoheiten erfordern eine praxisorientierte Planung, gute Organisation und klare Ziele. Ein Erfahrungsbericht am Beispiel eines Security Audits.

BILD: FOTOLIA

→ **VON SIMON WEPFER**

Die Aufgabe war klar: Ein internationaler Energiekonzern orderte vergangenen Frühling einen technischen Security Audit. Vier vom Internet aus erreichbare Netzwerke, unter anderem in Deutschland, Belgien und Grossbritannien sowie sechs ausgewählte Webapplikationen sollten auf Schwachstellen untersucht werden. Hunderte von Systemen einem intensiven Penetration Test zu unterziehen, macht allerdings aus Kostengründen wenig Sinn. Da die Systeme in der Regel über das Internet angegriffen werden, bot es sich an, auch das Testing über das Internet abzuwickeln. So wurde folgender Ablaufplan entwickelt: Die Netze sollten vorab automatisch gescannt werden – zunächst auf erreichbare Systeme, Protokolle und Ports, anschliessend auf Sicherheitslücken. Die so detektierten Risiken konnten dann manuell verifiziert werden, während im Hintergrund bereits der nächste automatisierte Test lief. Aufgrund der Ergebnisse wurden schliesslich zwölf Systeme ausgewählt, um sie einem intensiven Penetration Test zu unterziehen. Das Zeitfenster für die Tests: knappe drei August-Wochen.

Um diese enge Zeitvorgabe einhalten zu können, mussten die Ressourcen ortsübergreifend gebündelt werden: Teams aus Deutschland, Frankreich und der Schweiz wurden in den Prozess mit einbezogen. Das Projekt selbst war als Matrix organisiert und bestand aus den drei «Paketen» Security Scan, Penetration Test sowie Application Security Audit, jeweils mit einem eigenen Teilprojektleiter.

> Eine halbe Stunde nach Teststart war die erste Sicherheitslücke gefunden

Simon Wepfer ist COO bei der auf IT Security spezialisierten OneConsult GmbH

PHASE 1: KICK OFF ZUM PROJEKTSTART

Das Kick-off-Meeting, zehn Tage vor Projektstart, sollte dafür sorgen, dass jeder über Vorgehen, Zeitraum und Form der Tests informiert ist. Dort wurden die Kommunikationswege klar festgelegt und die Schlüssel zur sicheren Kommunikation ausgetauscht. Alle involvierten Personen wussten danach genau, was ihre Aufgabe im Projekt ist und wie die Eskalationspfade verlaufen. Weiter wurden rechtliche Aspekte geklärt, zum Beispiel, ob das Einverständnis der Systembetreiber vorliegt oder Geheimhaltungsvereinbarungen einzureichen sind.

An diesem «Initial Meeting» trafen IT-Bereichsleiter, Security Officer und CIO des Kunden mit den Projekt- und Teilprojektleitern sowie einem Vertreter aus der Geschäftsleitung zusammen. Da es für den Kunden nicht der erste technische Security Audit war, verlief das Treffen unkompliziert. Am Ende waren sämtliche Ziele erreicht, einzelne Aufgaben, etwa das Nachreichen weiterer Geheimhaltungsvereinbarungen, Genehmigungsanträge bei ISPs oder auch noch zu erstellende Accounts für die Webapplikationtests wurden in einer To-do-Liste mit Deadlines und Verantwortlichkeiten festgehalten.

PHASE 2: TESTVORBEREITUNGEN

Vor dem Start der Testphase fand noch ein internes Briefing statt. Um einen reibungslosen Projektablauf sicherzustellen, ist es wichtig, dass sämtliche Teilprojektleiter ihre Resultate in einer normalisierten Form einreichen. Falls die vom Kunden gewünschte Sprache des Schlussberichts nicht Englisch ist, und nicht alle Tester die Zielsprache beherrschen, muss auch der Aufwand für Übersetzungen der Ergebnisse und Beschreibungen berücksichtigt werden. In diesem Fall jedoch wünschte der Kunde einen englischen Bericht.

Aufgrund der lokalen Verteilung der Teams fand das Briefing auf zwei Ebenen statt: zunächst zwischen dem Projektleiter und den Teilprojektleitern, anschliessend zwischen Teilprojektleiter und Tester. Auf Letzterem wurden die Tagesziele definiert, die Tasks verteilt (z. B. wer testet wann welche Adressbereiche) sowie Inhalt, Ziel und Periode der Status-Updates festgelegt. Neben der Projektmanagement-Software hilft dabei ein Versionskontrollsystem, in dem jeder Tester täglich Resultate, Logs und Netzwerkmitschnitte speichert.

PHASE 3: DER ERSTE TAG

Wie beim Kick-off-Meeting festgelegt, holte sich der Projektleiter beim Kunden am ersten Testtag telefonisch das «Go» ab. Um administrativen Overhead zu vermeiden, waren die Tests ansonsten «opt-out» durchzuführen, das heisst, sie liefen automatisch während des vereinbarten Zeitfensters und konnten bei Bedarf vom Kunden gestoppt werden.

Während des Gesprächs wurde auch die To-do-Liste vom Kick-off-Meeting nochmals geprüft. Dabei stellte sich heraus, dass die schriftliche Erlaubnis zum Testen eines Routers trotz Nachhaken noch nicht eingetroffen war. Der besagte Router wurde also vorläufig ausgenommen und sollte nachgetestet werden, sobald die erwartete Erlaubnis eintraf. Eine halbe Stunde nach Projektstart fand das französische Testteam die erste Sicherheitslücke.

Es handelte sich um eine Anfälligkeit auf SQL-Injection. Die Eskalation verlief genau nach Plan: Der Tester meldete die Schwachstelle direkt seinem Projektleiter, der wiederum leitete umgehend eine kurze Beschreibung des Risikos inklusive konkretem Massnahmenvorschlag an den Projektleiter des Kunden weiter. Dieser kontaktierte daraufhin den Applikationsverantwortlichen aus Belgien, der das Problem innert weniger Stunden beheben liess. Die Nachkontrolle erfolgte noch am selben Tag – diese bestätigte, dass die Lücke korrekt geschlossen worden war.

PHASE 4: PROBLEMBEHEBUNG

Der weitere Projektverlauf lief nahezu problemlos ab: Die Erlaubnis für das Testen des Routers traf schliesslich doch noch ein, ein Benutzeraccount für die privilegierten Tests hatte falsche Berechtigungen, ein Passwort war falsch gesetzt und ein Intrusion Prevention System nicht korrekt konfiguriert, was die Inventur in einem Netz für etwa eine Stunde blockierte. Bei drei labilen Systemen wurden weitere Tests unterbrochen, da produktive Daten gefährdet waren und kein dediziertes Testsystem zur Verfügung stand.

PHASE 5: PROJEKTABSCHLUSS

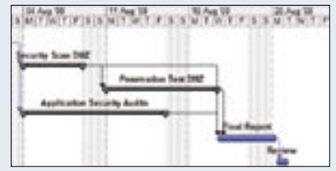
Nach Abschluss der Tests wurde der Schlussbericht erstellt. Auch hier lieferten die drei Teams ihre unabhängigen «Findings», die vom Teilprojektleiter stilistisch überarbeitet wurden. Alle drei Teilberichte wurden anschliessend vom Projektleiter zusammengefügt und kontrolliert. Das Resultat war ein 190-seitiger Bericht in Englisch, der neben einem Management Summary und organisatorischen Kapiteln eine Fülle von Risiken und Massnahmenvorschlägen enthielt. Nach der internen Qualitätssicherung wurde der Bericht schliesslich dem Kunden zugestellt.

Die Abschlusspräsentation fand zwei Wochen später statt: Der Kunde war mit Bericht und Projektablauf sehr zufrieden. Ohne die praxisorientierte Planung wäre ein Projekt dieser Grössenordnung, noch dazu unter Beteiligung eines internationalen Teams, wohl kaum für beide Seiten so reibungslos abgelaufen. ←

Checkliste → **Projekte**

Achten Sie bei internationalen Projekten auf folgende Punkte:

- → Rahmenbedingungen aufgrund unterschiedlicher Gesetzgebungen
- → Frühzeitiges Einholen notwendiger Einwilligungen
- → Klar definierte Kommunikationswege, sie verhindern Informationsabfluss und Doppelspurigkeiten
- → Standardisiertes Reporting von Schwachstellen und sämtlicher Infos für den Schlussbericht
- → Unterschiedliche Landessprachen
- → Reisekosten und Spesen



Klar definierte Projektschritte helfen, den Zeitplan einzuhalten