Daniel Hamburg

WIE SICHER SIND SIE, DASS SIE WIRKLICH SICHER SIND?

Die Sicherheit eines Webshops zu vernachlässigen, kann für den Anbieter fatale Folgen haben: Neben dem Image- und Reputationsschaden drohen ihm Vertragsstrafen und Sanktionen wegen Verstoßes gegen das Datenschutzgesetz. Dabei verspricht die Investition in IT-Security einen schnellen Return on Investment, denn sie schafft den im E-Commerce alles entscheidenden Wettbewerbsvorteil: das Vertrauen der Kunden.

DER AUTOR

Dr. Ing. Daniel Hamburg leitet das Security Engeneering bei TÜV Rheinland und ist seit über zehn Jahren in den Bereichen IT-Sicherheit und Datenschutz tätig.

Gefahren für Webshops und Online-Services

Viele Webshop-Betreiber und Anbieter von Online-Services gehen erstaunlich nachlässig mit dem Thema Sicherheit um. Dabei nehmen die Bedrohungen und Angriffe aus dem Internet permanent zu. Die Hacker sind oft technisch einen Schritt voraus und nutzen eine organisatorische interne Schwäche der Unternehmen aus: dass nämlich die Verantwortung für die verschiedenen Aspekte von Webshops und Portalen im Unternehmen oft in verschiedenen Händen liegt. Beispielsweise ist für die Inhalte der Marketingleiter zuständig, für die Informations- und Datensicherheit die IT-Abteilung, für den Umsatz (E-Commerce) der Vertrieb und für die Technik der technische Leiter.

Gerade im Bereich des E-Commerce ist aber die Vertrauenswürdigkeit im Wettbewerb um die Kunden der entscheidende Faktor. Und die Folgen einer Datenpanne sind fatal:

» Der Verlust von Kundendaten zerstört das Vertrauen der Kunden, das nur mühsam und langwierig wieder aufgebaut werden kann.
» Der Verlust von Unternehmensdaten schädigt das Image des Unternehmens so stark, dass es sich möglicherweise nie wieder davon erholt.
» Hinzu kommt ein möglicher Verstoß gegen das Datenschutzgesetz, der strafbar ist, mit Bußgeldern geahndet werden kann und gegebenenfalls öffentlich bekannt gemacht werden muss.

Unternehmen, die nicht für einen Datenschutz auf dem höchsten Stand der Technik sorgen, verlieren also nicht nur Umsatz und Reputation, sondern können sich auch strafbar machen.

Datenlecks aus jüngster Zeit

Dass nicht nur kleine und mittelständische Unternehmen Gefahr laufen, Opfer von Datendieben zu werden, zeigen einige Beispiele aus den letzten Wochen:

Beispiel eins

70 oder sogar 100 Millionen Datensätze von Privatpersonen entwendeten Unbekannte aus einer unverschlüsselten Datenbank mit den Personendaten der Nutzer: Namen, Anschriften, E-Mail-Adressen, Logins und Passwörter. Man kann davon ausgehen, dass dies ein profitorientierter Angriff war, denn allein die E-Mail-Adressen könnten Millionen einbringen, weil sie mit hoher Wahrscheinlichkeit echt sind und aktuell genutzt werden. Bei dem Einbruch wurden auch die Daten von 12,3 Millionen Kreditkarten entwendet, sogenannte „Kronjuwelen-Daten". Allein der Ersatz einer Kreditkarte kostet 20 Dollar.

Dem Unternehmen brachte diese Panne den Vorwurf der Schlamperei und Vertuschung ein – weil es seine Kunden erst eine Woche nach dem Einbruch informiert hatte – und hohe Schadensersatzklagen. Man kann heute noch nicht abschätzen, wie hoch der Schaden und möglicherweise die Vertrags- und Datenschutzstrafen sein werden, aber vermutlich handelt es sich um eine Summe in mindestens zweistelliger Millionenhöhe.

Beispiel zwei

Bei einem sozialen Netzwerk mit vielen Millionen Nutzern gab es eine Sicherheitslücke, die den Missbrauch von Daten möglich machte. Über Jahre konnten Dritte, insbesondere Werbekunden, auf die Profile von Mitgliedern zugreifen und private Daten wie Chatverläufe oder Fotoalben einsehen und sogar E-Mails im Namen der angemeldeten Nutzer verschicken.

Von dieser Panne waren Hunderttausende Mitglieder betroffen, die kleine Anwendungen (Apps) wie etwa Spiele oder Horoskope auf ihren Rechnern nutzten. Erst nachdem eine Sicherheitsfirma auf die Lücke hingewiesen hatte, wurde sie geschlossen. Sicherheitsexperten empfahlen den Nutzern, ihr Passwort zu ändern, um ihr Profil wieder sicher zu machen.

Methodik: Sicherheit in Online-Applikationen implementieren

Solche Fälle zeigen, dass Webshops und Online-Anwendungen in Gefahr sind, angegriffen und gehackt zu werden, wenn die Unternehmen keine Vorsorge treffen. Zu den prophylaktischen Maßnahmen gehört etwa, dass Passwörter für den Zugriff auf Nutzerdaten nur verschlüsselt abgelegt werden und alle Anwendungen ständig auf Lücken abgeklopft werden. Dies geschieht durch Sicherheitsanalysen, bei denen Experten Angriffe simulieren.

Für die Sicherheit von Online-Anwendungen gilt: Es ist nie zu früh und selten zu spät. Das typische Vorgehen bei der Schaffung von Sicherheit und Qualität für Webshops und Portale läuft in fünf Schritten ab: Konzept für Qualität und Sicherheit, Umsetzung und Betriebsunterstützung, Security-Analyse, Prüfung von Usability und Performance sowie Zertifizierung.

Mit Sinn und Verstand: Das Online-Sicherheitskonzept

Zunächst wird ein Sicherheitskonzept für die Infrastruktur, die Online-Applikationen und die datenschutzrelevanten Prozesse erstellt. Das Ziel ist, die potenziellen Gefahren zu identifizieren und entsprechende Gegenmaßnahmen zu planen. So hilft Verschlüsselung gegen den unbefugten Zugriff und die Manipulation von Kundendaten; Authentifizierungsmechanismen sorgen dafür, dass Angreifer keinen Zugriff auf Kundendaten erhalten und Kunden nur ihre eigenen Daten sehen können.

Häufig vernachlässigt wird die Sicherheit bei der Entwicklung neuer Online-Anwendungen. Die Berücksichtigung von Sicherheitsaspekten bereits bei der Erstellung des Software-Designs und während der Implementierung bietet jedoch doppelte Vorteile: Sie erspart eine oft kostspielige nachträgliche Beseitigung von Sicherheitslücken in der Software und die Wahrscheinlichkeit steigt,

dass die Applikation nicht nur heutigen, sondern auch zukünftigen Angriffen standhält.

Das Sicherheitskonzept wird an die Sicherheitspolitik (Security Policy) des Unternehmens angepasst und in das Informationssicherheitsmanagementsystem ISMS integriert.

Damit alles rund läuft: Umsetzung und Betriebsunterstützung

Der nächste Schritt ist die Umsetzung des Sicherheitskonzeptes. Dabei werden geeignete Maßnahmen ausgewählt, um die Sicherheit der Kundendaten zu gewährleisten. So helfen der Einsatz von Firewalls oder die Härtung von Server-Systemen , die Angriffsfläche von Online-Anwendungen zu verringern.

Damit sich nicht jeder Webshop-Betreiber zum Sicherheitsspezialisten weiterbilden muss, kann er auf Managed Services zurückgreifen. Das ist eine Art Rundum-Sorglos-Versicherung, bei der Fachleute aus dem Technical Assistance Center die Konfiguration und den Betrieb von Sicherheitskomponenten übernehmen, im Falle des Falles sicherheitsrelevante Hardware durch Ersatzgeräte austauschen und sich um das Lizenzmanagement sowie die Laufzeitkonsolidierung kümmern.

Managed Services bietet beispielsweise der TÜV Rheinland modular an, sodass ein Shop-Betreiber sich das Service Level Agreement SLA zu seiner individuellen Absicherung nach seinem eigenen Bedarf aussuchen kann. Fachleute für IT-Sicherheit haben meistens auch Finanzierungsmodelle im Angebot.

Auf dem Prüfstand: Die Sicherheitsanalyse

Die Sicherheitsanalyse deckt Risiken auf, die in der Applikation selbst und in den Applikationsdiensten liegen, und schlägt Maßnahmen vor, diese zu eliminieren oder auf ein akzeptables Maß zu reduzieren. Die Vorschläge orientieren sich beispielsweise an den Vorgaben der Standards ISO27001, IT-Grundschutz nach BSI und Open Web Application Security Project (OWASP).

Das aktuelle Sicherheitsniveau der Anwendung wird in drei Stufen analysiert: Bei Angriffen auf die zugrunde liegende Infrastruktur, bei Angriffen auf die Anwendung ohne gültige Benutzerkennung und bei Angriffen auf die Anwendung als authentifizierter Benutzer. Ziel ist die Überprüfung der Wirksamkeit bereits implementierter IT-Sicherheitsmaßnahmen und eine Steigerung der Sicherheit.

Im ersten Schritt werden die **IP-Adressen der Anwendung** auf Netzwerk- und Dienste-Ebene auf Schwachstellen untersucht. So werden sicherheitsrelevante Schwachstellen in der Firewall-Konfiguration und den erreichbaren Diensten identifiziert. Ferner wird festgestellt, ob das bestehende Patch-Management greift und die Serversysteme hinreichend gehärtet wurden.

Im zweiten Schritt wird versucht, die **Applikation ohne gültige Benutzerkennung** anzugreifen. Kann ein Angreifer den Login-Mechanismus bei administrativen Schnittstellen überwinden, zum Beispiel durch gezielte Brute-Force-Angriffe (Standard-Benutzerkennungen und Passwortlisten mit Standard- und Trivialpasswörten)? Wie verhält sich die Anwendung bei Parameter-Veränderungen, etwa mit Fehlermeldungen, die auf potenzielle Schwachstellen hindeuten? Was passiert bei einer Änderung an Session-Variablen und Cookies, bei Datenbankangriffen wie SQL-Injection oder anderen Manipulationen? Wie reagiert die Applikation auf Cross-Site-Scripting , Code- und Command-Injection-Angriffe ? Weitere Angriffsvarianten hängen von der jeweiligen Programmiersprache und Technologie der Anwendung ab.

Im dritten Schritt wird die **Anwendung von einem authentifizierten Benutzer** angegriffen. Dies simuliert einen Angreifer, der Zugriff auf die Login-Daten eines Benutzers hat. Ein solcher interner Angreifer hat viel mehr Möglichkeiten als ein Angreifer von außen: Kann er etwa auf die Daten anderer Benutzer zugreifen? Kann er Kontrolle über die Applikation oder sogar über andere Systeme erhalten? Untersucht werden die Reaktion der Applikation auf Änderungen an Session-Variablen und Cookies und die Zuverlässigkeit beziehungsweise Nicht-Vorhersagbarkeit der Session. Zusätzlich wird geprüft, ob nicht-öffentliche Teile der Applikation ohne vorherige Authentifizierung erreichbar sind.

Auf Biegen und Brechen: Usability und Performance

Neben den Sicherheitsaspekten spielen die Benutzerfreundlichkeit und die Schnelligkeit der Applikation eine Rolle. Sind die Daten der Benutzer vielleicht so sicher, dass nicht einmal der Benutzer sie einsehen kann? Verlässt jeder zweite Benutzer den Webshop aus Verzweiflung, da er nicht das findet, was er sucht? Experten untersuchen die Usability der Applikationen und helfen, sie so zu gestalten, dass der Benutzer sich wohlfühlt und mit möglichst wenig Klicks direkt zum

gewünschten Ziel kommt.

Muss ein Benutzer zu lange auf die Applikation warten, wenn mehr als zehn Benutzer gleichzeitig zugreifen? Last- und Performanz-Tests simulieren typisches Anwenderverhalten und -aktionen und messen die Reaktion der Applikation und ihre Antwortzeiten.

Die Krönung: Das Zertifikat

Das Tüpfelchen auf dem i ist ein Zertifikat für den Webshop, denn es bedeutet geprüfte Sicherheit und schafft eine breite Vertrauensbasis. Noch unbekannte Anbieter von Online-Applikationen können mit einem Zertifikat einen Vertrauensvorschuss erreichen, den sie sich sonst in jahrelanger Arbeit aufbauen müssten. Bereits etablierte Webshop- und Portal-Betreiber festigen und bestätigen mit einem Zeugnis das bereits bestehende Vertrauen ihrer Kunden.

» Das Zertifikat „Datenschutz und Datensicherheit“ des TÜV Rheinland etwa bestätigt dem Anwender, dass die organisatorischen, administrativen und datenschutzrelevanten Prozesse der Online-Applikation mit technischen Sicherheitsanalysen untersucht wurden.

» Das Zertifikat „Geprüfter IT-Testprozess“ des TÜV Rheinland bescheinigt die Auditierung des Software-Qualitätssicherungsprozesses bereits während der Entwicklung.

Ergebnis: Dem Wettbewerb eine Nasenlänge voraus

Mit der Implementierung von Sicherheitsmechanismen in ihre Online-Applikationen steigern die Anbieter die Qualität der Services und verschaffen sich somit Wettbewerbsvorteile. Sie sparen sogar Kosten ein, denn Fehler frühzeitig zu erkennen und zu beheben ist immer preiswerter, als für einen bereits entstandenen Schaden aufkommen zu müssen. Nebenbei erschließen sie sich Verbesserungspotenziale.

Die objektive Risikobewertung durch einen unabhängigen Experten gewährleistet, dass Gesetze und Richtlinien eingehalten werden (Compliance) und bestätigt die Betriebssicherheit und Skalierbarkeit. Last, but not least helfen sichere Online-Anwendungen, die Produktivität zu erhöhen.

Kurz: Sicherheit erhöht das Vertrauen der Kunden, dies führt zu mehr Besuchen Ihrer Kunden auf der Website, zu einer höheren Konversionsrate und damit zu mehr Umsatz.¶