SONICWALL

KURZDARSTELLUNG: WARUM DIE WEBANWENDUNGSSICHERHEIT WICHTIG IST

Die speziellen Risiken von Business-Websites

Zusammenfassung

Webanwendungen sind aus modernen Unternehmen nicht mehr wegzudenken, doch gleichzeitig bergen sie erhebliche Risiken. Diese Kurzdarstellung befasst sich mit potenziellen webbasierten Exploits und Angriffen, um die sich die IT kümmern muss, wie zum Beispiel:

- Code-Injection/Remote-Code-Inclusion
- Cross-Site-Scripting(XSS)-Schwachstellen
- Web-Session-Hijacking
- unzureichende Authentifizierung und Autorisierung

Einleitung

In einer anwendungsbasierten Welt sind Webapplikationen – speziell für Organisationen, die sich in einem global umkämpften Digital-Business-Umfeld bewegen – ein wichtiger Enabler. Dazu gehören die Bereiche Markenpflege, Werbung und Kundenakquisition. Unternehmen, Institutionen und Behörden stehen ständig unter Druck, Innovationen voranzutreiben und nützliche Webanwendungen zu entwickeln, um das unstillbare Verlangen der Nutzer nach einem sofortigen Zugriff auf Informationen, Services und Support zu erfüllen.

Die rasante Zunahme von Webanwendungen in Unternehmen

Mehr als die Hälfte[1] der Weltbevölkerung nutzt heute das Internet. 93 Prozent[1] aller Internetnutzer gehen mit ihren Mobilgeräten ins Netz und surfen damit vielleicht länger im Internet als mit ihren Computern. Durch das Internet der Dinge (Internet of Things, IoT) kommen zusätzlich mehrere Milliarden[2] Geräte hinzu, die über Webanwendungen und mobile Applikationen vernetzt sind, miteinander kommunizieren und Daten austauschen – angefangen bei Fernsehern, digitalen Wearables, Fahrzeugen, Spielekonsolen und Vending-Units bis hin zu allen möglichen intelligenten Geräten (Smart Appliances).

Organisationen versuchen, das bestmögliche Serviceerlebnis und ein hohes Kundenengagement über verschiedene Typen interaktiver Webapplikationen und benutzerfreundlicher mobiler Anwendungen sicherzustellen. Daher sind Webanwendungen heute

unverzichtbarer denn je. Unternehmen müssen darauf achten, dass diese Applikationen jederzeit mit dem Internet verbunden sind und zuverlässig geschützt werden.

Sicherheitsbedenken

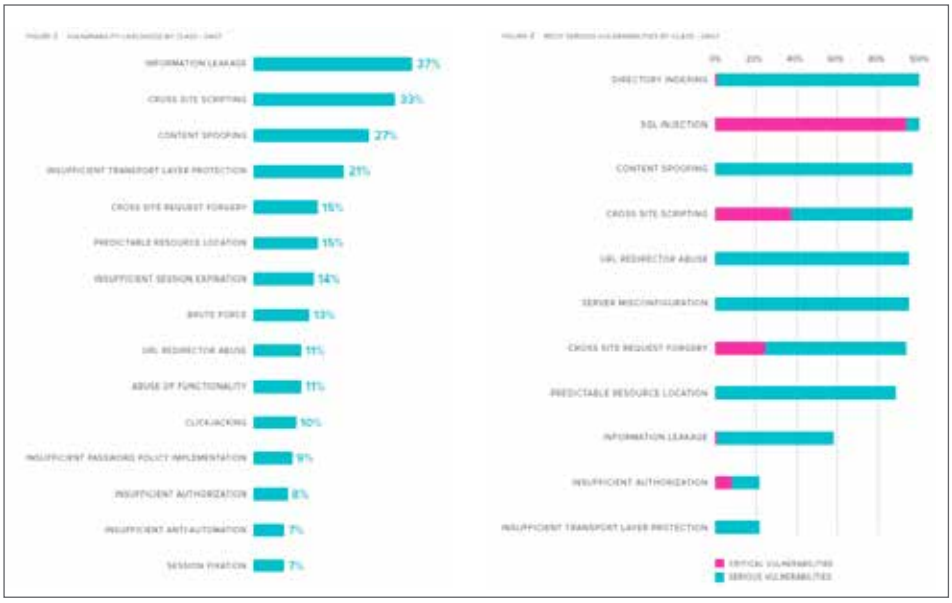
Wenn eine Webanwendungssoftware am selben Ort implementiert wird wie die Daten, auf die sie zugreifen muss, wird sie allerdings schnell zu einem gefährlichen Sicherheitsrisiko. Das rührt daher, dass sie einen potenziellen Einstiegspunkt für Angreifer darstellt, die solche Daten stehlen möchten oder sich einen weiteren Zugriff auf sensiblere Teile des Netzwerks verschaffen wollen. Mit jeder Webanwendung, die Organisationen implementieren, steigt das Risiko, Opfer einer großen Bandbreite potenzieller webbasierter Exploits und Angriffe zu werden.

Einem vor kurzem erschienenen Bericht zufolge[3] sind knapp 50 Prozent der Webanwendungen das ganze Jahr über durchgehend anfällig für Angriffe. Zu diesen empfindlichen Schwachstellen zählen Datenlecks (37 %), Cross-Site-Scripting (33 %), Content-Spoofing (27 %), unzureichender Schutz der Transportschicht (21 %) und Cross-Site-Request-Forgery (15 %). Betrachtet man die Auswirkungen auf das Unternehmen, so gilt SQL-Injection als schwerwiegendste Schwachstelle, gefolgt von Cross-Site-Scripting (XSS), Cross-Site-Request-Forgery (XSFR) und unzureichender Autorisierung.

Diese Zahlen zeigen: Ernste Qualitätsprobleme beim Quellcode sowie Sicherheitsprobleme lassen sich auch künftig bei Webanwendungen nicht ausschließen. Webentwicklern gelingt es anscheinend immer noch nicht, die nötigen Sicherheitspraktiken bei der Entwicklung von Code umzusetzen. So meint Gartner:[4] „Entwickler werden weiterhin unsicheren Code erstellen, und es gibt nichts, was sie dagegen tun können. Der Kampf, den sie sich mit Hackern liefern, ist einfach aussichtslos."

Compliance-Daten sind aufgrund mangelhafter Webentwicklungsprozesse sowie unzureichender Sicherheitspatches gefährdet. Unternehmen sind deshalb nicht in der Lage, gesetzliche Sicherheitsvorgaben wie PCI, HIPPA und die DSGVO einzuhalten. Regelmäßig werden Softwareschwachstellen in Anwendungen wie Contentmanagementsystemen (CMS), Foren und Portalen, die von großen wie kleinen Organisationen in allen Industrien genutzt werden, gemeldet und auch von Hackern ausgenutzt.

Verschärft wird dieses Problem durch die Nutzung zahlreicher Protokolle in Webanwendungen – wie HTTP(S), JSON, XML und SOAP – sowie durch uneingeschränkte und offene Benutzerschnittstellen (UIs). Webanwendungen sind auch in der Zeitspanne gefährdet, in der Organisationen auf Systempatches von internen und/oder externen Softwareentwicklern warten.



Angriffsszenarien

Lassen Sie uns als Beispiel einen Blick auf ein typisches Webformular werfen, das mithilfe einer gängigen Webentwicklungssprache wie JavaScript oder PHP erstellt wurde.

Dieses Formular akzeptiert diverse Parameter für die Webanwendungen, um die gesammelten Informationen zu verarbeiten. Verfügt die Anwendung nicht über Sicherheitsfunktionen – wie etwa die Prüfung und Validierung von Eingangsdaten – können Angreifer möglicherweise die Anwendung ausnutzen und den Service kompromittieren, indem sie beliebigen Content in das Formular eingeben.

In diesem Szenario können Angreifer mittels einer oder mehrerer gängiger PHP-Anwendungsschwachstellen ihren eigenen Code in die Webanwendung einfügen. Diese Art von Attacke wird typischerweise Local- oder Remote-Code-Inclusion-Angriff genannt.

Gängige Webserver hosten heute mehrere Webanwendungen auf einem einzigen Host und sind über einen einzigen Port zugänglich (Port 80 für HTTP und 443 für HTTPS). Für Organisationen stellt dies eine breite Angriffsfläche dar, die sie verteidigen müssen.

Fazit

Unternehmen können sich nicht darauf verlassen, dass ihr Webentwicklungsteam fehlerlose Webanwendungen bereitstellt. Ein Blick auf die hohe Anzahl versuchter Webangriffe – pro Jahr zwischen Hunderttausenden und mehreren Millionen – zeigt, dass IT-Administratoren das Thema Sicherheit selbst in die Hand nehmen müssen.

Erfahren Sie mehr. Lesen Sie unsere Lösungsübersicht Best Practices für Web-Application-Firewalls oder besuchen sie uns unter www.sonicwall.com/web-application-firewall.

[1] https://thenextweb.com/contributors/2017/04/11/current-global-state-internet/
[2] https://cdn.ihs.com/www/pdf/IoT-ebook.pdf
[3] https://info.whitehatsec.com/rs/675-YBI- 674/images/WHS%202017%20Application%20Security%20Report%20FINAL.pdf
[4] https://sdtimes.com/automation/stop-fighting-yesterdays-software-security-wars/

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, Kalifornien 95035, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com