Akamai

WHITEPAPER

Die Top 10 von OWASP

Wie Akamai zum Schutz vor weit verbreiteten Sicherheitslücken beiträgt

Einführung

Die Top-10-Liste von OWASP (Open Web Application Security Project) umfasst die häufigsten Schwachstellen von Webanwendungen und schafft so mehr Bewusstsein bei Unternehmen. Wenn Sie die wirksamsten Maßnahmen zum Schutz gegen die Top 10 der OWASP-Sicherheitslücken umsetzen wollen, müssen Sie verstehen, an welchen Stellen, auf welche Weise und in welchem Umfang Sicherheitsanbieter Sie bei der Verbesserung Ihrer eigenen Entwicklungspraktiken unterstützen können. In der folgende Aufschlüsselung der Top-10-Schwachstellen von OWASP wird jede davon beschreiben und es wird erläutert, wie Akamai Unternehmen durch Edge-Sicherheitslösungen, Managed Services und die weltweit größte Intelligent Edge Platform unterstützen kann.

Akamai-Produkte

Top 10 der OWASP-Sicherheitsrisiken		Account Protector	Akamai Guardicore Segmentation	App & API Protector	Bot Manager	Enterprise Application Access	Enterprise Threat Protector	Identity Cloud	Managed Security Services	Akamai MFA	Page Integrity Manager
Schwachstellen bei der Zugriffssteuerung	A01			✓	✓	✓		✓		✓	
Kryptografische Fehler	A02			✓		✓	✓				✓
Injection	A03			✓							
Nicht sicheres Design	A04			✓		✓					
Fehlerhafte Sicherheitskonfiguration	A05		✓	✓	✓						
Anfällige und veraltete Komponenten	A06		✓	✓							✓
Fehlgeschlagene Identifizierungs- und Authentifizierungsversuche	A07	✓		✓	✓	✓		✓		✓	
Software- und Datenintegritätsfehler	A08		✓	✓			✓				✓
Fehler bei der Sicherheitsprotokollierung und -überwachung	A09		✓	✓		✓	✓		✓		
Server-Side Request Forgery	A10		✓	✓							

Bei den Top 10 von OWASP handelt es sich um Risikokategorien, nicht um Einzelrisiken. Die Lösungen von Akamai handhaben diese Risikokategorien auf verschiedene Arten. Weitere Informationen erhalten Sie im Whitepaper.

A01: Schwachstellen bei der Zugriffssteuerung

> "Durch Zugriffskontrolle wird eine Richtlinie umgesetzt, so dass Nutzer nicht außerhalb ihrer vorgesehenen Berechtigungen handeln können. Fehler führen in der Regel zu einer unbefugten Offenlegung, Manipulation oder Zerstörung aller Daten oder zur Durchführung einer Geschäftsfunktion außerhalb der Berechtigungen des Nutzers."
>
> – Quelle: owasp.org

Was Akamai-Lösungen bewirken

Um die Schwachstelle der beschädigten Zugriffskontrolle vollständig zu beheben, müssen Sie die Fehler in Ihrem Zugriffssteuerungsmodell beseitigen. Akamai bietet Ihnen mit Fachwissen im Bereich WAAP Hilfe bei der Erkennung einiger der Angriffsvektoren, damit Sie sich dagegen schützen können:

- **Enterprise Application Access** bietet Unternehmensnutzern ein Zugriffsmodell der geringstmöglichen Berechtigungen, sodass nur authentifizierte Nutzer Sichtbarkeit und Zugriff auf autorisierte Anwendungen erhalten. Dies entspricht dem Zero-Trust-Sicherheitsmodell.
- **Akamai MFA** bietet starke Authentifizierungsservices, die auf phishing-resistenten FIDO2-Technologiestandards basieren.
- **App & API Protector** – die WAAP-Lösung von Akamai – durch die Überprüfung des „Referer"-Headers dazu beitragen, erzwungene Browser-Angriffe zu blockieren und die Authentifizierung für APIs erzwingen, um die Zugriffskontrolle mit Akamai API Gateway zu verbessern.
- **Identity Cloud** umfasst fein abgestimmte Zugriffskontrollen für Endnutzerdaten und ermöglicht so den Zugriff mit den geringstmöglichen Berechtigungen für jeden internen Nutzer oder jedes interne System.
- **Bot Manager** verhindert automatisierte Angriffe mit Tools und Angriffe mit Anmeldeversuchen.

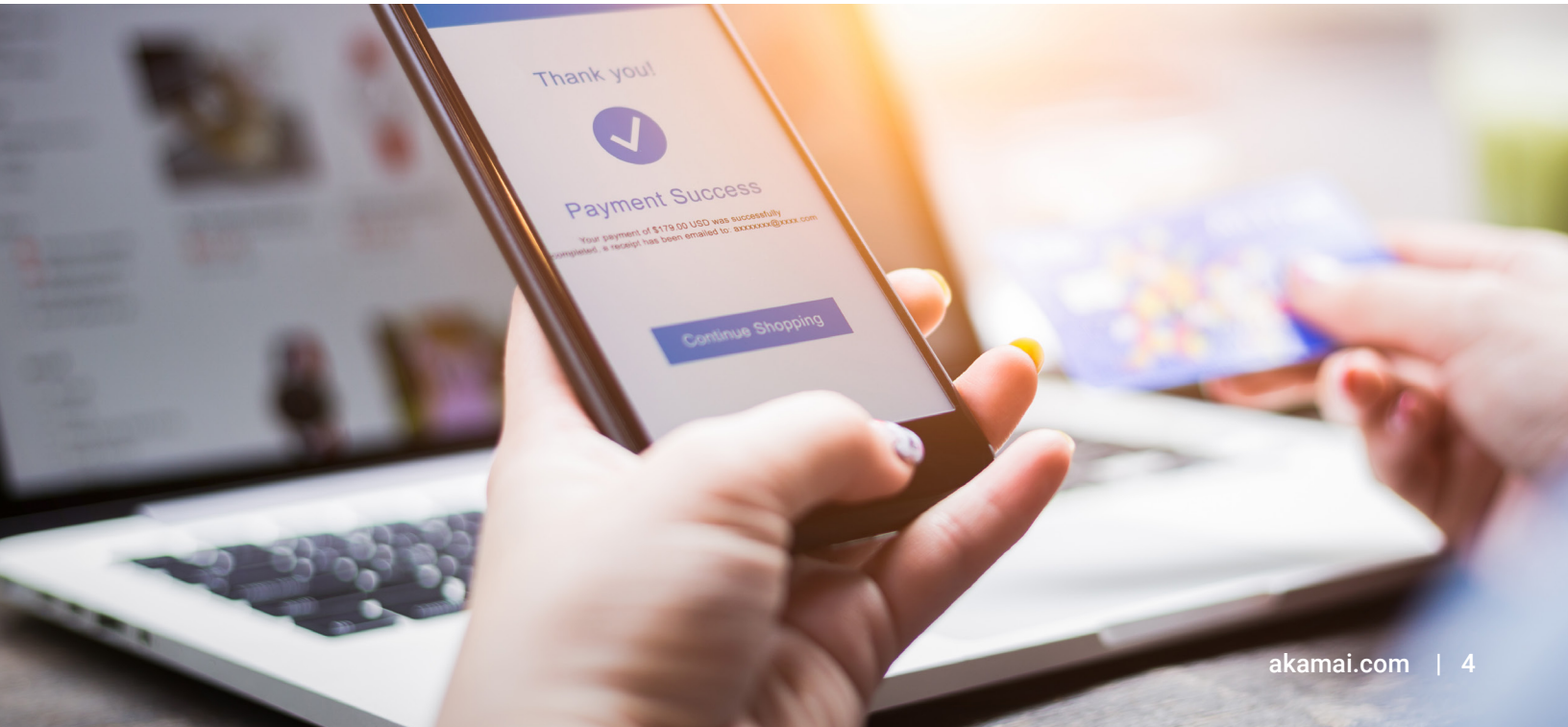
A02: Kryptografische Fehler

> „Der Fokus liegt auf Fehlern im Zusammenhang mit Kryptographie (oder dem Fehlen von Kryptographie). Dies führt häufig zur Offenlegung sensibler Daten. … Zum Beispiel erfordern Passwörter, Kreditkartennummern, Krankenakten, persönliche Informationen und Geschäftsgeheimnisse zusätzlichen Schutz. Vor allem, wenn diese Daten Datenschutzgesetzen unterliegen.“
>
> – Quelle: owasp.org

Was Akamai-Lösungen bewirken

Unternehmen können sich nicht vollständig gegen kryptografische Fehler schützen, indem sie auf eine einzige Sicherheitslösung setzen. Eine Kombination aus verschiedenen Lösungen kann jedoch zumindest einige Aspekte dieser Schwachstelle beheben. Akamai bietet beispielsweise folgende Lösungen:

- **App & API Protector** verschlüsselt und schützt sensible Daten während der Übertragung mit den neuesten Versionen von TLS und starken Verschlüsselungsverfahren. Er trägt auch dazu bei:
  - Die PCI-Compliance aufrechtzuerhalten, da sich die Server ausschließlich in einem sicheren CDN befinden, das alle markenspezifischen TLS-Zertifikate unterstützt und die privaten Schlüssel eines Kunden schützt.
  - Ein CDN zu bieten, das durch sowohl durch betriebliche als auch physische Sicherheitsmaßnahmen wie abgeschlossene Racks und Bewegungsmelder geschützt ist, sodass nur autorisiertes Personal auf die Server zugreifen kann.
  - Mit API PII Learning Stellen zu finden, an denen sensible Daten verlorengehen und dies zu vermeiden.
- **Enterprise Application Access** macht den Remotezugriff sicher, indem die Kommunikation verschlüsselt und vertrauliche Daten im Netzwerk vor neugierigen Blicken verborgen werden.
- **Enterprise Threat Protector** kann dazu beitragen, die Offenlegung sensibler Daten zu verhindern.
- **Page Integrity Manager** kann auch PII-Datenverluste durch den Missbrauch von JavaScript-Code erkennen, der möglicherweise auf kryptografische Fehler zurückzuführen ist.



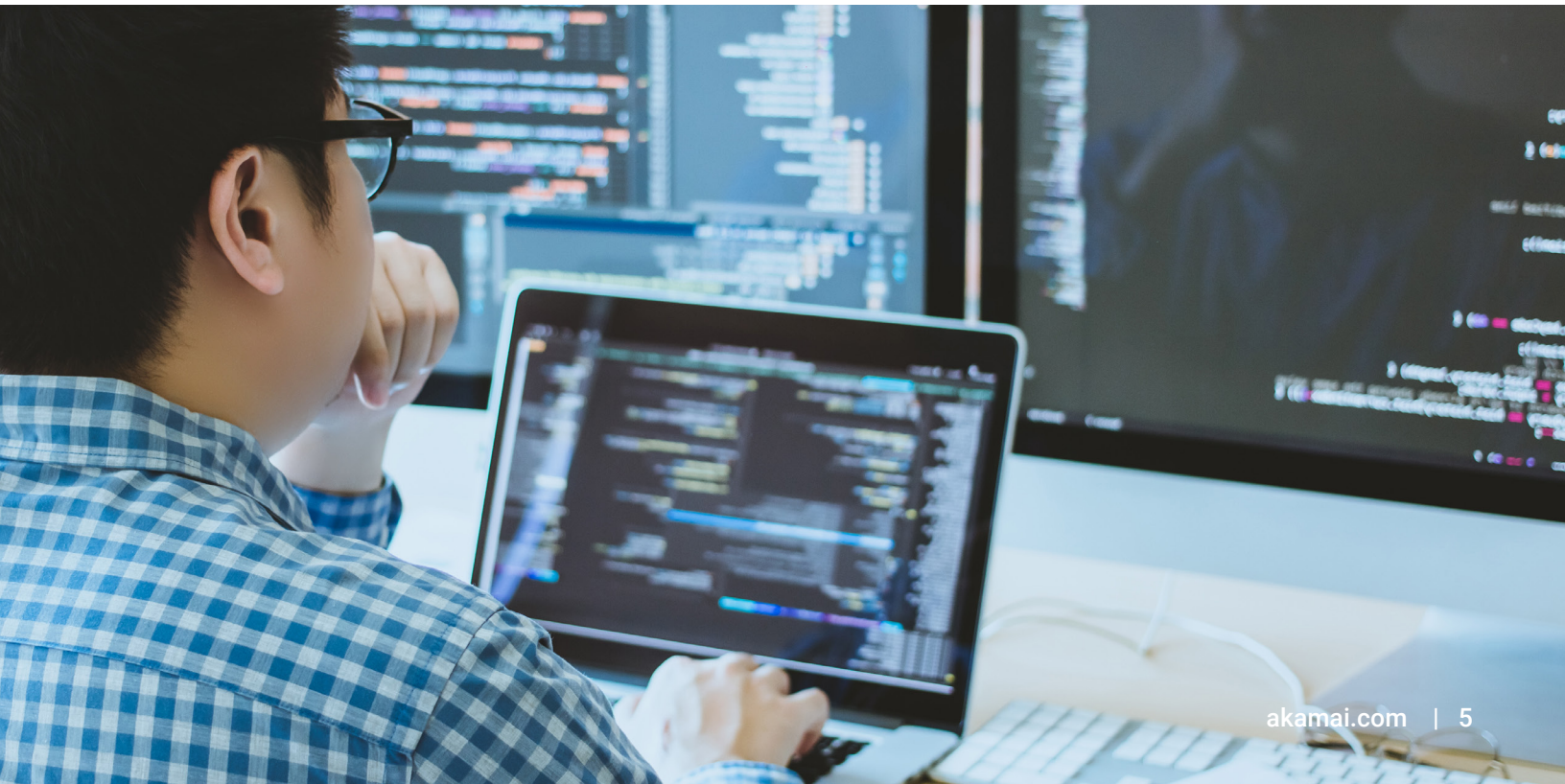
A03: Injection

> „Injection-Bedrohungen wie beispielsweise SQL-, NoSQL-, Betriebssystem- und LDAP-Injections treten auf, wenn nicht vertrauenswürdige Daten als Teil eines Befehls oder einer Abfrage an einen Interpreter gesendet werden. Die schädlichen Daten des Angreifers können den Interpreter dazu verleiten, Befehle auszuführen oder Datenzugriff ohne entsprechende Autorisierung zuzulassen.“
>
> – Quelle: Akamai

Was Akamai-Lösungen bewirken

Sie können WAAP nutzen, um das Risiko durch Injection-Sicherheitslücken bei Webanwendungen und API zu verringern. Unternehmen sollten Webanwendungen immer patchen, um erkannte Schwachstellen im Rahmen des jeweiligen Entwicklungslebenszyklus zu beheben.

- **App & API Protector** ist eine branchenführende WAAP-Lösung mit einer Adaptive Security Engine (ASE), die mit fertig vorkonfigurierten Regeln einen umfassenden Schutz vor Injection-Angriffen bietet. Die ASE-„Strafbank“ kann mit WAAP vorübergehend den gesamten Traffic von Clients blockieren, die kürzlich einen Injection-Angriff versucht haben.
- Dank virtuellem Patching mit nutzerdefinierten Regeln können entstehende Injection-Schwachstellen oder neue Sicherheitslücken, die durch Anwendungsänderungen auftreten, schnell beseitigt werden, bis das Programm gepatcht werden kann. Sicherheitsorganisationen können zudem virtuelles Patching automatisieren und es in DevSecOps-Prozesse integrieren, indem sie die Akamai-API-Funktionen nutzen.
- **Client Reputation** kann dazu beitragen, Injection-Angriffe zu erkennen und abzuwehren und zeigt eine Risikobewertung für hochaktive schädliche Clients in der Kategorie „Webangreifer“.



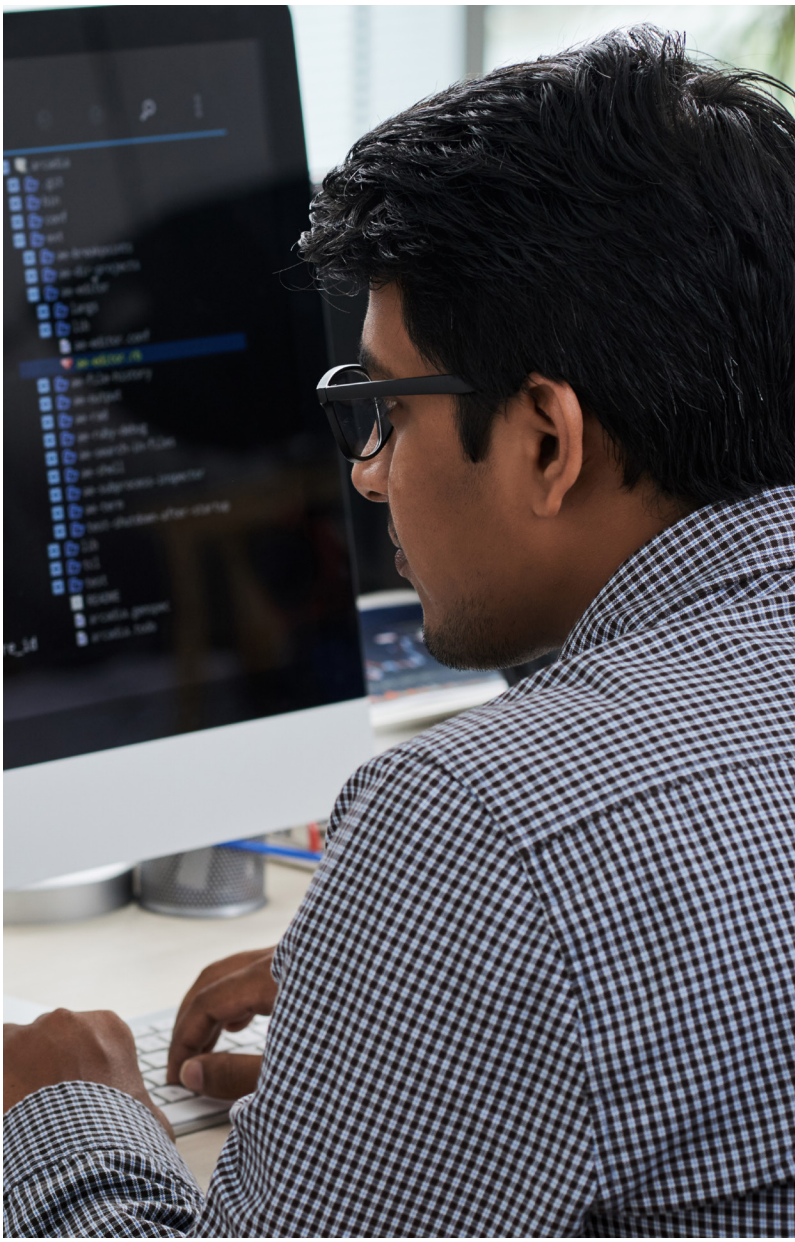
A04: Nicht sicheres Design

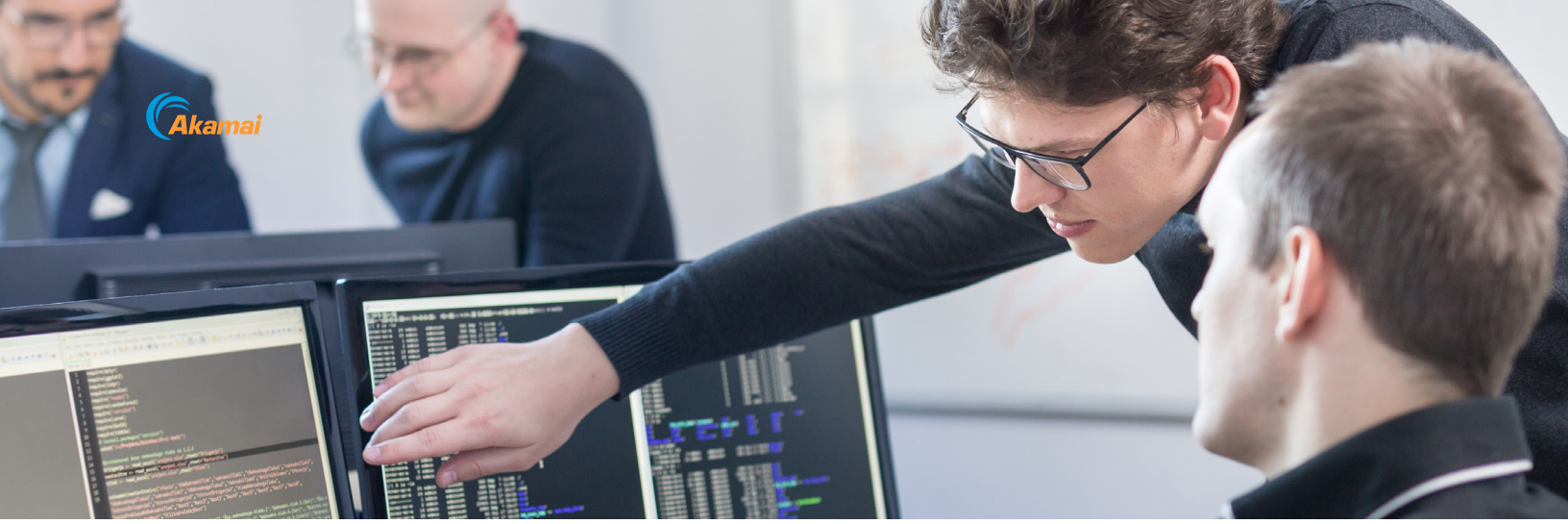
> „Nicht sicheres Design ist eine breite Kategorie, die verschiedene Schwachstellen umfasst, die als ‚fehlendes oder ineffektives Kontrolldesign' in Erscheinung treten. Es gibt einen Unterschied zwischen nicht sicherem Design und nicht sicherer Implementierung. Ein sicheres Design kann immer noch Implementierungsfehler aufweisen, die zu Schwachstellen führen. Ein nicht sicheres Design kann nicht durch eine perfekte Implementierung behoben werden, da per definitionem die erforderlichen Sicherheitskontrollen zur Abwehr spezifischer Angriffe nie geschaffen wurden."
>
> – Quelle: owasp.org

Was Akamai-Lösungen bewirken

Unternehmen sollten bereits in den ersten Designphasen Sicherheitslösungen integrieren. Allerdings können Entwicklungsteams Schwierigkeiten haben, dies zu erreichen, wenn die Integration von Sicherheitslösungen umständlich ist. Mit den Produkten von Akamai können Unternehmen ihre IT-Anwendungen und APIs schneller verschieben, um zu verhindern, dass Unsicherheitsfaktoren im Design sie gefährden.

- **App & API Protector** – mit unserer WAAP-Lösung und ASE – kann auch einige Designfehler, die während der Produktionsphase noch bestehen, erkennen und beheben. Darüber hinaus nutzt die Lösung die Automatisierung, um Routineaufgaben zu optimieren und zu vereinfachen, sodass nur diejenigen, die eine menschliche Analyse erfordern, von Menschen erledigt werden. Diese Automatisierung umfasst automatische Updates, Selbstoptimierung, API-Erkennung, vereinfachte Programmierbarkeit und das Nutzererlebnis.
- **Enterprise Application Access** garantiert, dass nur autorisierte Nutzer auf Anwendungen zugreifen können. Dieser Ansatz der geringstmöglichen Berechtigungen verhindert laterale Netzbewegungen zu anderen Anwendungen, was bei Netzwerkzugriffslösungen wie VPNs leicht passieren kann.





A05: Fehlerhafte Sicherheitskonfiguration

> „[Seit] der vorherigen Ausgabe wurden 90 % der Anwendungen auf irgendeine Form von Fehlkonfiguration getestet, mit einer durchschnittlichen Inzidenzrate von 4 % und über 208.000 Fällen von Common Weakness Enumeration (CWE) in dieser Risikokategorie. Ohne einen koordinierten, wiederholbaren Konfigurationsprozess für die Anwendungssicherheit sind Systeme einem höheren Risiko ausgesetzt.“
>
> – Quelle: owasp.org

Was Akamai-Lösungen bewirken

Fehlerhafte Sicherheitskonfiguration betrifft per definitionem mehrere Aspekte der Anwendungssicherheit. Außerdem müssen Unternehmen Sicherheitskontrollen angemessen konfigurieren. Akamai-Produkte können Sie folgendermaßen unterstützen:

- **App & API Protector** ist zwar kein Ersatz für eine angemessene Konfiguration, kann aber durch folgende Aspekte nützlich sein:
  1. Er umfasst Angriffsgruppen für Anomalien bei ausgehenden Daten, um Datenlecks wie Fehlercodes sowie Quellcode zu erkennen, der auf fehlerhafte vorhandene Standard-Sicherheitskonfigurationen zurückzuführen ist.
  2. Er stellt Regeln zum Erkennen und Stoppen von XXE-Angriffen auf, die greifen, bevor der XML-Parser die gefährliche externe Entität verarbeitet.
  3. Er stellt Regeln auf, die den Zugriff auf bekannte sensible Dateien, die von Entwicklern auf den Produktionsservern abgelegt wurden, erkennen.
- **Akamai Guardicore Segmentation** schützt vor Datenverlusten durch Fehlkonfigurationen, indem es Transparenz und Einzelfallüberwachung jeder nicht autorisierten oder ungeplanten Kommunikation zwischen Ihren Anwendungen und dem Internet bietet.
- Virtuelles Patching mit nutzerdefinierten Regeln trägt dazu bei, erkannte Datenverluste schnell zu beheben, bis Ihr Team die Anwendung gepatcht hat.
- Mit **App & API Protector** und **Bot Manager** können Brute-Force-Angriffe über Standardanmeldeinformationen durch Ratensteuerungen geschützt werden.
- Die Akamai-Plattform verbessert die Sicherheit, wenn die Header der Inhaltssicherheitsrichtlinie und andere sicherheitsrelevante Header eine schwache Sicherheitskonfiguration aufweisen.
- Mit der automatischen API-Erkennung in **App & API Protector** können Sie Ihre APIs automatisch und kontinuierlich erkennen und ein Profil erstellen, einschließlich Endpunkten, Definitionen sowie Ressourcen- und Traffic-Eigenschaften.

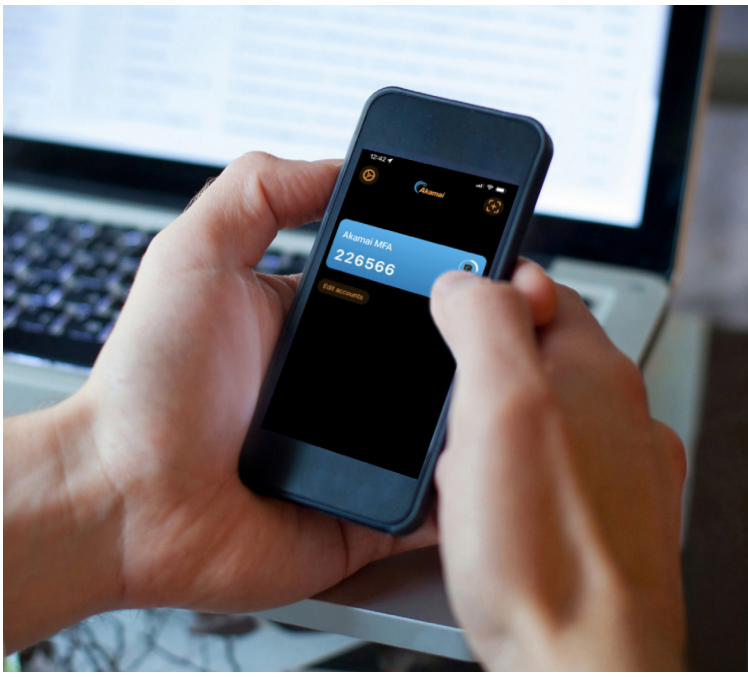
A06: Anfällige und veraltete Komponenten

> „Komponenten wie Bibliotheken, Frameworks und andere Softwaremodule werden mit denselben Berechtigungen wie die Anwendung ausgeführt. Außerdem fungieren Skripte als vertrauenswürdige Anwendungsressourcen mit uneingeschränktem Zugriff auf Anwendungsdaten. Wenn eine anfällige Komponente ausgenutzt wird, kann der resultierende Angriff einen schwerwiegenden Datenverlust oder eine Serverübernahme zufolge haben.“
>
> – Quelle: Akamai

Was Akamai-Lösungen bewirken

Unternehmen verlieren leicht den Überblick und die Sicherheitsteams wissen oft gar nicht, welche Komponenten von Drittanbietern in ihren Anwendungen existieren. Darüber hinaus haben Unternehmen keine Kontrolle darüber, wie schnell, wenn überhaupt, der Drittanbieter neu entdeckte Schwachstellen behebt. Um diesen Mangel an Transparenz und Sicherheit zu beheben, ist der Einsatz einer Sicherheitslösung wie WAAP sowie Skriptschutz erforderlich. Wie etwa:

- **App & API Protector** umfasst mehrere Regeln, die speziell auf bekannte Schwachstellen abgestimmt sind. Dabei kann es sich um Schwachstellen in Ihren eigenen Anwendungen oder in Komponenten von Drittanbietern handeln. Er bietet außerdem API-Schutzfunktionen, die APIs auch dann schützen, wenn Komponenten von Drittanbietern, die in die API integriert sind, sie für Missbrauch anfällig machen.



- Mit dem Insight-Modul von **Akamai Guardicore Segmentierung** können Sie in Ihrem Netzwerk nach Assets suchen, die möglicherweise gefährdet sind. Die integrierte Einzelüberprüfung ermöglicht es außerdem, alle betroffenen Ressourcen so lange zu beschränken, bis ein Patch durchgeführt wurde.
- Dank virtuellem Patching mit nutzerdefinierten Regeln können entstehende Schwachstellen oder neue Sicherheitslücken, die durch Anwendungsänderungen auftreten, schnell beseitigt werden, bis das Programm gepatcht werden kann.
- **Client Reputation** bietet Risikobewertungen für schädliche Clients der Kategorie „Web-Scanning“ zum Schutz vor der Ausnutzung neuer Schwachstellen.
- **Page Integrity Manager** analysiert permanent das Verhalten der Skriptausführung in Sitzungen mit echten Nutzern, um verdächtiges oder offen schädliches Verhalten zu identifizieren. Er blockiert auch die Datenexfiltration aus Skripten des Unternehmens und von Drittanbietern in URLs mit bekannten Schwachstellen mithilfe einer CVE-Datenbank (Common Vulnerabilities and Exposures), die ständig aktualisiert wird.

A07: Fehlgeschlagene Identifizierungs- und Authentifizierungsversuche

> „Anwendungsfunktionen im Zusammenhang mit Authentifizierung und Sitzungsverwaltung werden oft nicht ordnungsgemäß implementiert. Dadurch können Angreifer Passwörter, Schlüssel oder Sitzungstoken kompromittieren oder andere Implementierungsfehler ausnutzen, um die Identitäten anderer Nutzer vorübergehend oder dauerhaft zu stehlen.“
>
> – Quelle: Akamai

Was Akamai-Lösungen bewirken

Unternehmen müssen ihre eigenen Lücken schließen, um diese Sicherheitsanfälligkeit vollständig zu beheben. Doch auch die unten aufgeführten Akamai-Lösungen können dazu beitragen, viele der Angriffsvektoren zu erkennen und abzuwehren, die versuchen, fehlgeschlagene Identifizierungs- und Authentifizierungsversuche auszunutzen:

- **Bot Manager** kann automatisierte Angriffe, wie sie beispielsweise bei Credential-Stuffing-Angriffen verwendet werden, erkennen und abwehren.
- **Account Protector** reduziert Kontoübernahmen, bei denen Betrüger versuchen, unbefugten Zugriff auf Nutzerkonten zu erhalten.
- **Enterprise Application Access** kann den Zugriff auf Anwendungen über ein „Zugriffsmodell mit geringstmöglichen Berechtigungen“ approximieren, wodurch die Angriffsfläche der Anwendung reduziert und der Zugriff verbessert wird.
- **Akamai MFA** bietet eine starke Authentifizierung mithilfe der phishing-resistenten FIDO2-Technologie.
- **App & API Protector** bietet eine Ratensteuerung, mit der Brute-Force-Angriffe abgewehrt werden können.
- **Identity Cloud** bietet eine sichere Verwaltung von Anmeldedaten und Profilinformationen für Endnutzer, die durch zwei-Faktor-Authentifizierung und Funktionen zur risikobasierten Authentifizierung geschützt sind.

A08: Software- und Datenintegritätsfehler

> „Software- und Datenintegritätsfehler beziehen sich auf Code und Infrastruktur, die nicht vor Integritätsverletzungen schützt. Ein Beispiel dafür ist, dass eine Anwendung auf Plugins, Bibliotheken oder Module aus nicht vertrauenswürdigen Quellen, Repositorys und Content Delivery Networks (CDNs) angewiesen ist. Eine nicht sichere CI/CD-Pipeline birgt das Potenzial für unbefugten Zugriff, schädlichen Code oder Systemmanipulationen.“
>
> – Quelle: owasp.org

Was Akamai-Lösungen bewirken

Unternehmen können WAAP verwenden, um Webanwendungen und APIs vor Software- und Datenintegritätsfehlern zu schützen. Unternehmen sollten Webanwendungen immer patchen, um erkannte Schwachstellen im Rahmen des Entwicklungslebenszyklus zu beheben.

- **App & API Protector**
  - bietet starken Schutz vor Deserialisierungsangriffen.
  - Setzt auf Implementierung der neuesten TLS-Versionen und starker Verschlüsselungen und verhindert so Man-in-the-Middle-Angriffe, die zu Problemen mit der Datenintegrität führen können.
  - Setzt auf Implementierung von DNSSEC mit Edge DNS und gewährleistet die Datenursprungsauthentifizierung und den Schutz der Datenintegrität der DNS-Einträge. So wird die Manipulation von DNS-Einträgen verhindert, durch die Nutzer zu nicht vertrauenswürdigen Quellen geleitet werden können.
- Mit dem Insight-Modul in **Akamai Guardicore Segmentation** können Sie in Ihrem Netzwerk nach allen Assets suchen, die das manipulierte Update erhalten haben. Die integrierte Einzelüberprüfung ermöglicht es außerdem, die betroffenen Ressourcen so lange zu beschränken, bis eine Reparatur durchgeführt wurde.
- **Enterprise Threat Protector** erkennt Phishing-Angriffe, die Administratoren und Superuser der Anwendungen in gefährliche Umgebungen oder zu nicht vertrauenswürdigen Quellen locken können.
- Virtuelles Patching mit nutzerdefinierten Regeln hilft, neue Deserialisierungsschwachstellen schnell zu beheben, bis die Anwendung gepatcht werden kann.
- **Page Integrity Manager** erkennt Skripte von Drittanbietern, überwacht sie auf Veränderungen und ergreift dann Maßnahmen für Skripte, die manipuliert wurden.

A09: Fehler bei der Sicherheitsprotokollierung und -überwachung

"Unzureichende Protokollierung, Erkennung, Überwachung und zu schwache Reaktionen treten jederzeit auf:

- Prüfereignisse, wie z. B. Anmeldungen, fehlgeschlagene Anmeldungen und hochwertige Transaktionen, werden nicht protokolliert.
- Warnungen und Fehler erzeugen keine, unzureichende oder unklare Protokollmeldungen.
- Protokolle von Anwendungen und APIs werden nicht auf verdächtige Aktivitäten überwacht.
- Protokolle werden nur lokal gespeichert.
- Geeignete Schwellenwerte für Warnmeldungen und Eskalationsprozesse für Reaktionen sind nicht vorhanden oder ineffektiv.
- Penetrationstests und Scans durch DAST-Tools (Dynamic Application Security Testing) lösen keine Warnungen aus.

Die Anwendung kann aktive Angriffe nicht in Echtzeit oder annähernd Echtzeit erkennen, eskalieren oder einen Alarm auslösen."

– Quelle: owasp.org

Was Akamai-Lösungen bewirken

Bei der Sicherheitsprotokollierung und -überwachung handelt es sich um eine Unfähigkeit eines Unternehmens, Schwachstellen zu beheben. Akamai bietet zahlreiche Funktionen, um Unternehmen einen besseren Einblick in Angriffe zu ermöglichen. U. a. sind folgende Punkte Teil des Angebots:

- Akamai stellt Dashboards und Reporting-Tools in der grafischen Nutzeroberfläche des Akamai Control Center zur Verfügung.
- Akamai-Produkte für den Anwendungsschutz lassen sich in die vorhandene SIEM-Infrastruktur des Unternehmens integrieren, um von Akamai erkannte Vorfälle mit denen anderer Sicherheitsanbieter in Beziehung zu setzen.
- **Managed Security Service** bietet Analyse- und Reaktionsfunktionen rund um die Uhr.
- **App & API Protector** umfasst eine „Strafbank"-Funktion, die eine verstärkte Protokollierung verdächtiger Sitzungen zur weiteren gründlichen Analyse ermöglicht.
- **Enterprise Application Access** bietet eine integrierte Identitätsverwaltungslösung zur Authentifizierung und Steuerung des Zugriffs auf alle Unternehmensanwendungen. Bei der Kombination mit der identitätsbasierten Proxyfunktion erhalten Unternehmen detaillierte Einblicke in Nutzeraktionen bis hin zu allen GET-/POST-Vorgängen.
- **Enterprise Threat Protector** ermöglicht vollständige Sichtbarkeit aller externen – sowohl schädlichen als auch harmlosen – DNS-Anfragen von einem Unternehmen.
- **Akamai Guardicore Segmentation** bietet einen tiefen Einblick in den Kommunikationsfluss in Ihrem Netzwerk, sodass Warnungen gesendet werden können, wenn eine nicht autorisierte oder unerwartete Kommunikation stattfindet. Außerdem können Sicherheitsrichtlinien bis hin zu individuellen Prozessen oder bis auf die Service-Ebene durchgesetzt werden, um diese Kommunikation einzuschränken. Mit dem zusätzlichen Modul zur Erkennung von Angriffen können potenzielle Bedrohungen schnell erkannt und behoben werden.

A10: Server-Side Request Forgery

> "SSRF-Fehler treten auf, wenn eine Webanwendung eine Remote Ressource abruft, ohne die vom Nutzer eingegebene URL zu validieren. Das ermöglicht einem Angreifer, die Anwendung zu zwingen, eine manipulierte Anfrage an ein unerwartetes Ziel zu senden, auch wenn es durch eine Firewall, VPN oder eine andere Art von Access Control List (ACL) für das Netzwerk geschützt ist."
>
> – Quelle: owasp.org

Was Akamai-Lösungen bewirken

Akamai WAAP enthält Regeln, die nach URL-Injections suchen können. Diese Funktion kann verhindern, dass Angreifer den Server dazu bringen, zu einem anderen Ort zu wechseln und eine Anfrage zu senden, damit sie wie eine gültige Anfrage an Ihre Sicherheitsanalysten aussieht.

- Die Regeln von **App & API Protector** verhindern, dass diese Exploit-Anfragen den anfälligen Server überhaupt erreichen.
- **Akamai Guardicore Segmentation** kann unerwarteten ausgehenden Traffic auf Serverebene überwachen und blockieren.

Fazit

Um den besten Schutz gegen die Top 10 der größten Schwachstellen laut OWASP zu gewährleisten, müssen Unternehmen und ihre Sicherheitsanbieter zusammenarbeiten, um Schwachstellen so schnell wie möglich aufzudecken und Lösungen zu implementieren, um sich zu schützen. Erfahren Sie mehr über das Akamai-Edge-Sicherheitsportfolio. Wenn Sie mehr darüber erfahren möchten, wie wir als Partner den bestmöglichen Schutz für Ihr Unternehmen bereitstellen können, nehmen Sie bitte Kontakt mit Ihrem Akamai-Vertriebsmitarbeiter auf.