

Trend Micro™

Web Application Security

Schützen Sie Ihre Website vor Cyber-Angriffen und Datenverlust.

Unternehmen sind heutzutage auf die Verfügbarkeit ihrer umsatzgenerierenden Webanwendungen angewiesen, um Kunden, Lieferanten, Mitarbeiter und Partner rund um die Uhr miteinander zu verbinden. Jedoch sind Angriffe auf Websites auf dem Vormarsch, und die Anforderungen zur Einhaltung von Datenschutzrichtlinien werden immer komplexer. Um Ihre Internet-Präsenz und Ihr Unternehmen zu schützen, müssen Sie Ihre Schwachstellen erkennen und beheben. Trend Micro ermöglicht Ihnen den Zugriff auf kritische Informationen, mit denen Sie Angriffe von Cyber-Kriminellen auf Ihre Website verhindern können.

Web Application Security unterstützt Sie beim Schutz Ihrer Websites, bevor Ihre Systeme infiziert werden. Dazu überprüft die Lösung die Computer nach Sicherheitslücken und erstellt ausführliche Wiederherstellungsberichte. Diese Berichte weisen den Wiederherstellungsaktivitäten Prioritäten zu, so dass Sie schnell Schwachstellen in der Host- oder Anwendungsschicht Ihrer Website beheben können. Zwischen den Suchvorgängen überprüft Web Application Security Ihre Website mit Hilfe des Trend Micro Smart Protection Network auf Anhaltspunkte für Angriffe. Ergibt sich dabei, dass sich auf Ihrer Website bösartige Inhalte befinden, werden Sie umgehend benachrichtigt, damit Sie die notwendigen Gegenmaßnahmen ergreifen können, um Schaden für Ihre Unternehmenswerte und Ihren Ruf abzuwenden.

DIE WICHTIGSTEN FUNKTIONEN

Schwachstellenbewertung

- Durchsucht Ihre Website automatisch oder manuell nach Internet-Bedrohungen und Schwachstellen
- Wartet automatisch die aktuellen Schwachstellenbibliotheken und Wiederherstellungsdaten
- Durchsucht mit Hilfe von Web-Crawler-Technologien eine Vielzahl von Webanwendungen, wie beispielsweise die neuesten Web-2.0-Anwendungen
- Beinhaltet Expertensysteme und Pass-Through-Suchmethoden, um Fehlalarme zu reduzieren und Schwachstellen noch gründlicher zu untersuchen

Suche nach Richtlinienverstößen (demnächst verfügbar)

- Erkennt Schwachstellen und damit verbundene Risiken in einer Vielzahl von Webanwendungen, Datenbanken, Netzwerken, Betriebssystemen, kommerziellen Anwendungen und anderen Software-Produkten
- Liefert präzise Suchergebnisse in kürzerer Zeit durch den Einsatz von Verfahren, die auch seriöse Hacker verwenden
- Fördert die Einhaltung von Richtlinien wie PCI, Sarbanes-Oxley und HIPAA (Healthcare Insurance Portability and Accountability Act)

Qualifizierte Berichte

- Stellt Zusammenfassungen und Wiederherstellungsberichte mit minutengenauen Informationen von TrendLabsSM bereit, dem weltweiten Netzwerk von Sicherheitsexperten
- Führt Risikodaten in einem zentralen Bericht zusammen und stuft diese nach deren

- Gefahrenpotenzial ein. So erhalten Sie ein vollständiges Bild über die Sicherheitsrisiken, damit Sie schnell reagieren können
- Liefert umfassende Daten über Schwachstellen in Form standardisierter Berichte, in denen die richtigen Informationen in der für Ihr Unternehmen erforderlichen Genauigkeit enthalten sind

Wiederherstellungstipps

- Ermöglicht Administratoren, Schwachstellen anhand der Informationen in den Wiederherstellungsberichten schnell und einfach zu beheben
- Unterstützt Sie dabei, Ihren IT-Sicherheitsprojekten Prioritäten zuzuweisen und den Zeitaufwand für die Behebung von Schwachstellen zu minimieren

Überwachung und Warnmeldungen bei Angriffen

- Überwacht rund um die Uhr das Trend Micro Smart Protection Network, das nach Anhaltspunkten für eine Infektion Ihrer Website sucht
- Warnt Sie sofort, wenn Ihre Websites angegriffen werden oder sich darauf bösartige Inhalte befinden
- Erlaubt die schnelle Wiederherstellung Ihrer Website und verhindert, dass Besucher Ihrer Website geschädigt werden oder unwissentlich Spam verbreiten

Service mit Vertrauenssiegel

- Bietet optional die Auszeichnung mit dem SecureSite Vertrauenssiegel zum Nachweis der Sicherheit für Besucher Ihrer E-Commerce-Site
- Schützt Ihre E-Commerce-Websites vor Hackern und bösartigen Bedrohungen

GEHOSTETER SUCH-SERVICE

Geschützte Punkte

- Webanwendungen
- Netzwerksysteme
- Gehostete Betriebssysteme

Durchsuchte Schwachstellen

- Web 2.0 (JavaScript, AJAX, Flex)
- Cross-Site-Scripting
- SQL-Injection
- Ermöglicher von Betrug und Phishing
- Unbefugte Nutzung
- Veraltete Host-Patches

ÜBERWACHUNGSSERVICE

- Unterstützt durch das Smart Protection Network
- Erkennung bösartiger Inhalte
- Warmmeldungen bei Angriffen

ENTSCHEIDENDE VORTEILE

- Reduziert Zeitaufwand, Risiko und Kosten für das Erkennen und Beheben von Sicherheitslücken
- Behebt potenzielle Sicherheitsprobleme, bevor Schaden für Ihr Unternehmen entsteht
- Hilft bei Aufbau und Wartung starker Datensicherheit durch den Schutz weborientierter Systeme und Anwendungen
- Vermeidet Kosten für Erwerb und Wartung mehrerer Produkte
- Erleichtert die Verteilung durch die Bereitstellung als "Software-as-a-Service"
- Bietet Rund-um-die-Uhr-Unterstützung durch ein weltweites Netzwerk von Datenzentren

KEINE KOSTEN FÜR ERWERB UND WARTUNG VON SICHERHEITSSYSTEMEN

Als webbasierter Service wird Web Application Security vollständig über das Trend Micro Online-Netzwerk betrieben. Sie bestimmen, wann und wie (automatisch oder manuell) die Suche nach Sicherheitslücken durchgeführt wird. Die Ergebnisse erhalten Sie über ein nicht öffentliches Webportal. Installation, Konfiguration, Erwerb von Hardware, Software-Entwicklung, Sicherheitsexpertise, spezielle Schulungen und neue Technologien werden überflüssig. Bei unserer Software-as-a-Service-Lösung müssen Sie nur Ihre Unternehmensdomains und IP-Adressen an Trend Micro weiterleiten – um den Rest kümmern wir uns. Trend Micro stellt Ihnen sein Fachwissen im Bereich Malware-Erkennung und Suche nach den neuesten Sicherheitslücken bereit. Unsere umfassende Knowledge Base wird automatisch mit den neuesten Informationen aktualisiert und reduziert dadurch das Risiko einer Infektion für Sie auf ein Minimum.

DURCHSUCHT	BEISPIELE	SCHÜTZT VOR
Anwendungsschicht	<p>Webinfrastruktur: Apache, Apache Tomcat, Microsoft™ Internet Explorer, Mozilla FireFox, Microsoft™ IIS, FTP, BEA Weblogic, Adobe ColdFusion, SSH, TELNET und Warenkörbe</p> <p>Web 2.0: JavaScript, AJAX, Adobe Flash Anwendungen</p> <p>Webanwendungen: Anwendungen und Content auf der Website</p>	<ul style="list-style-type: none"> • Angriffe auf Websites durch Ausnutzung von Computer-Schwachstellen mit Hilfe von Cross-Site-Scripting (XSS) • Content-Spoofing • Javascript-Schadteile • Schwachstellen, die einen Denial-of-Service-Angriff auf Websites verursachen können • Beschädigung oder Entwendung von Daten und Identitäten
Datenbanken	<ul style="list-style-type: none"> • Oracle • Microsoft™ SQL Server • Sybase • PostgreSQL • Sun™ MySQL • IBM™ DB2 • IBM™ DB2/400 • Lotus Notes™/Lotus™ Domino™ 	<ul style="list-style-type: none"> • SQL-Injection-Angriffe, die auf die Entwendung von Kreditkartendaten und Identitäten abzielen • Konfigurationsprobleme und Richtlinienverstöße
Netzwerkssysteme	Cisco™ Firewalls, IPSec, PPTP, Network File System (NFS), DHCP, DNS, LDAP, SNMP	<ul style="list-style-type: none"> • Probleme in der Systemkonfiguration (z. B. schwache Kennwörter) • Unbefugter Zugriff auf Systeme
Betriebssysteme	Microsoft™ Windows™, Linux, UNIX, Sun™ Solaris™, Mac OS, BSC, IBM™ AIX™, IBM™ AS/400, Novell™ NetWare™	Zu- oder Angriff auf ein Betriebssystem durch Richtlinienverletzungen, wie z. B. vorhersehbare Kennwörter, Dateiberechtigungen oder unangemessenen Kontozugriff

SYSTEMVORAUSSETZUNGEN

Um den ordnungsgemäßen Betrieb der Weboberfläche sicherzustellen und Berichte anzuzeigen, benötigen Benutzer von Web Application Security eine Internet-Verbindung und einen der folgenden Browser:

- Microsoft Internet Explorer 6 oder höher
- Mozilla Firefox 1.5.x oder höher

* http://news.zdnet.com/2424-1009_22-198647.html

ERWEITERN SIE IHREN SCHUTZ

- InterScan™ Web Security Virtual Appliance
- ServerProtect
- InterScan Messaging Hosted Service

ANGRIFFE AUF WEBSITES AUF DEM VORMARSCH

- Über 79 % der Websites, auf denen sich bössartiger Code befindet, sind seriöse Websites, die durch Hacker manipuliert wurden (ZDNet, April 2008*)
- 50 % der Online-Shops weisen schwerwiegende Sicherheitslücken auf (TrendLabs, 2008)
- Über 28.000 bekannte XSS-Schwachstellen (Cross-Site-Scripting) auf namentlich erwähnten Websites entdeckt, wovon nur 5 % behoben wurden (www.xssed.com, August 2008)



©2008 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro T-Ball-Logo, InterScan, TrendLabs und Worry-Free sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- oder Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer. [DS01WAS_081111DE]

www.trendmicro.com