

Trend Micro™ SecureSite

Schützen Sie Ihre E-Commerce-Website, sichern Sie Ihre Online-Umsätze, und bewahren Sie die Daten Ihrer Kunden vor Hackern, Viren und Identitätsdiebstahl.

E-Commerce-Websites erzielen Umsätze, repräsentieren das Image einer Marke und vermitteln dem Kunden einen ersten Eindruck des Unternehmens. Ein Hacker kann jedoch Schwachstellen auf seriösen Websites ausnutzen und das Unternehmen dadurch unwissentlich zum Komplizen für Spyware oder Identitätsdiebstahl machen. Geschäftsumsätze, Kundendaten und der Ruf des Unternehmens wären in Gefahr.

Trend Micro™ SecureSite ist eine gehostete, webbasierte Lösung, mit der Online-Händler oder Web-Hosting-Firmen Websites einmal täglich automatisch nach Schwachstellen durchsuchen und Berichte erstellen können. Werden Schwachstellen gefunden, können Online-Händler ihre eigenen IT-Mitarbeiter oder Trend Micro Channel Partner mit der Behebung des Problems beauftragen. Unterstützt werden sie hierbei von den Sicherheitsexperten des weltweiten TrendLabsSM Netzwerks. Durch diesen Online-Service ist keine zusätzliche Software oder Hardware nötig, die verteilt, installiert oder gewartet werden muss.

Der SecureSite Service durchsucht Websites täglich nach Schwachstellen, gefährlichen Inhalten und Links, die PCs und vertrauliche Daten der Kunden dem Missbrauch aussetzen. Als Teil der Service-Leistung erhalten Websites, die die Sicherheitsrichtlinien erfüllen, ein neues Trend Micro SecureSite Vertrauensiegel, woran Internet-Nutzer erkennen, dass der Betreiber der Website dem Thema Sicherheit ausreichend Bedeutung beimisst.

DIE WICHTIGSTEN FUNKTIONEN

SecureSite Überwachung

- Durchsucht Ihre Website jeden Tag automatisch nach Internet-Bedrohungen und Schwachstellen
- Stärkt das Vertrauen Ihrer Kunden in die Sicherheit und den Schutz ihrer Daten
- Schützt den Ruf des Unternehmens
- Schützt Schwachstellen auf E-Commerce-Websites mit der branchenführenden Technologie von Trend Micro

Sichere Webanwendungen mit Trend Micro

- Bewertet die Sicherheit einer Website durch tägliche Schwachstellen-Snapshots und schützt dadurch vor Website-Hijackern, SQL Injection, Cross-Site-Scripting, Bot-Aktivitäten und anderen Angriffen
- Durchsucht eine Vielzahl von Webanwendungen, Datenbanken und Betriebssystemen nach Schwachstellen
- Meldet die am meisten gefährdeten Schwachstellen, damit Sie schnell die richtigen Prioritäten setzen können
- Bietet eine webbasierte Konsole mit einer Zusammenfassung aller Schwachstellen und einer Auswahl von Alarmpoptionen
- Gibt Tipps für IT-Experten zum Umgang mit einer ständig wachsenden Anzahl von Sicherheitslücken, damit auftretende Probleme schnell behoben werden können

Keine Installation von Hardware oder Software erforderlich

- Von Trend Micro gewartet und aktualisiert, damit Sie jederzeit von den neuesten Technologien und Schutzfunktionen profitieren können

SICHERE WEBANWENDUNGEN ZUM SCHUTZ VON ONLINE-HÄNDLERN

SecureSite sucht automatisch einmal am Tag nach folgenden Arten von Schwachstellen:

Möglichkeiten für Betrug und Phishing

Cross-Site-Scripting ermöglicht Phishing-Betrug und ist die häufigste Schwachstelle auf Websites.

Datenlecks

Datenlecks können Angreifern den Zugriff auf vertrauliche Daten, wie z. B. IP-Adressen, Sozialversicherungsnummern, Kreditkartendaten, interne Webseiten, Quellcode und XML-Dokumente, ermöglichen.

Unbefugte Nutzung

Durch die unbefugte Nutzung der Website oder ihrer Infrastruktur können Angreifer auf geschützte Bereiche der Website zugreifen, Benutzer belästigen, zur Preisgabe vertraulicher Daten verleiten oder sogar die Kontrolle über die Server übernehmen.

DIE ZAHLEN BEWEISEN: WEBSITES BRAUCHEN LÜCKENLOSEN SCHUTZ

- Über 28.000 bekannte XSS-Schwachstellen auf namentlich erwähnten Websites entdeckt, wovon nur 5 % behoben wurden – www.xssed.com, August 2008
- Über 40 % aller Internet-Bedrohungen befanden sich auf seriösen Websites, die unwissentlich Malware verteilten – **TrendLabs, 2008**
- Über 70 % der Online-Kunden achten beim Besuch einer Website auf ein Gütesiegel eines unabhängigen Dritten – **Kundenberichte**¹



Tested: 2 Sept, 2008

SOFTWARE UND SERVICES

Geschützte Punkte

- Internet-Anwendungen
- Datenbanken
- Netzwerke
- Betriebssysteme

Durchsucht Websites, um vor folgenden Schwachstellen zu schützen:

- Hacker-Angriffe
- Web-Bedrohungen
- Javascript-Malware
- Ermöglicher von Betrug und Phishing
 - Cross-Site-Scripting
- Datenlecks
 - Informationslecks
 - Vorhersehbare Weblinks
 - Directory Traversal
 - XPath Injection
- Unbefugte Nutzung
 - Unzureichende Befugnis
 - Funktionsmissbrauch
 - Pufferüberlauf

ENTSCHEIDENDE VORTEILE

- Schützt E-Commerce-Websites vor Hackern und bössartigen Bedrohungen
- Hilft Ihnen, den Ruf Ihres Unternehmens zu schützen, das Vertrauen Ihrer Kunden zu erhalten und Ihre Online-Umsätze zu sichern
- Erkennt Schwachstellen und bietet Expertenlösungen
- Unterstützt E-Commerce-Unternehmer bei der Einhaltung der Payment Card Industry Security (PCI DSS) Auflagen
- Ermöglicht ein ungestörtes Einkaufserlebnis im Internet

SICHERE WEBANWENDUNGEN ZUM SCHUTZ VON ONLINE-HÄNDLERN

SecureSite ist ein von Trend Micro gehosteter und gewarteter Service. Ohne Installation zusätzlicher Soft- oder Hardware durchsucht der Service unter anderem folgende Versionen von Webanwendungen, Datenbanken, Netzwerk- und Betriebssystemen nach Risiken und Schwachstellen.

DURCHSUCHT	BEISPIELE	SCHÜTZT VOR
Web- und Web-2.0-Anwendungen	<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 das Ausnutzen von Computer-Schwachstellen mit Hilfe von Cross-Site-Scripting • Content-Spoofing • Schadteile mit Javascript-Malware • Schwachstellen, die zu einem Denial-of-Service-Angriff auf Websites führen 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 Identitätsdiebstahl abzielen • Konfigurationsprobleme und Verletzung von Richtlinien
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 Richtlinienverstöße, wie z. B. leicht zu erratende Kennwörter, Dateiberechtigungen oder unerlaubten Kontozugriff

SYSTEMVORAUSSETZUNGEN

Um den ordnungsgemäßen Betrieb der Weboberfläche sicherzustellen, benötigen Benutzer eines SecureSite Kontos eine Internet-Verbindung und einen der folgenden Browser:

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

¹ <http://www-03.ibm.com/press/us/en/pressrelease/19154.wss>, 25. Januar 2006.

² IDC, Worldwide Antivirus 2006-2010 Forecast Update und 2005 Vendor Analysis, Dokumentennr. 204715, Ausgabe 1, Dezember 2006.

³ Results of Anti-Spam Solution Testing, Opus One, Februar 2007.

⁴ Gartner Magic Quadrants for Enterprise BI Suites and Platforms von B. Hostmann, et al. 28. Februar 2008.

Der Gartner Magic Quadrant wurde am 28. Februar 2008 von Gartner Inc. durch Copyright geschützt und wird in diesem Dokument mit freundlicher Genehmigung genutzt. Der Magic Quadrant ist eine grafische Darstellung eines Marktes während eines bestimmten Zeitraums und stellt die Analyseergebnisse von Gartner bezüglich marktspezifischer Kriterien von Anbietern dar. Gartner unterstützt weder einen der im Magic Quadrant dargestellten Anbieter, dessen Produkte oder Services, noch empfiehlt das Unternehmen speziell einen der Anbieter im Quadranten „Leaders“. Der Magic Quadrant hat ausschließlich informativen Charakter und soll nicht als Aufforderung verstanden werden, einem bestimmten Anbieter den Vorzug zu geben. In Zusammenhang mit dieser Untersuchung übernimmt Gartner keinerlei vertragliche oder gesetzliche Gewährleistung und gewährt keinerlei Zusicherungen allgemeiner oder erforderlicher Gebrauchstauglichkeit.

NUR DAS BESTE FÜR SIE: TREND MICRO

- Marktführer im Bereich wirksamer Schutz vor Spam³
- Marktführer im Bereich Email Reputation Services
- Größte vernetzte Reputationsdatenbank
- Spitzenposition im "Magic Quadrant for Endpoint Protection Platforms" von Gartner⁴

ONLINE-RESSOURCEN

- www.worryfree.com

ERWEITERN SIE IHREN SCHUTZ

PC-, Server- und E-Mail-Sicherheit

- Worry-Free Business Security

Gehostete E-Mail-Sicherheit

- InterScan™ Messaging Hosted Security

Services

- Rund-um-die-Uhr-Support



©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 ihrer jeweiligen Eigentümer. [DS03SecureSite080822DE]
<http://de.trendmicro.com>