

Trend Micro™ – Häufig gestellte Fragen (FAQ)

Trend Micro Web Application Security

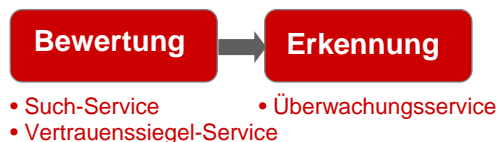
Häufig gestellte Fragen:

1. Was ist die Trend Micro Web Application Security Lösung?
2. Warum muss ich meine Websites vor Angriffen schützen?
3. Wie können Malware oder Hacker meine Website und mein Unternehmen schädigen?
4. Wie weiß ich, ob Web Application Security die richtige Lösung für mein Unternehmen ist?
5. Was bedeutet das SecureSite Vertrauenssiegel?
6. Wie kann Trend Micro feststellen, ob meine Website angegriffen wurde?
7. Kann ich Trend Micro Web Application Security testen?
8. Wie funktioniert der Web Application Security Service?
9. Welche Arten von Web-Anwendungskomponenten durchsucht Web Application Security?
10. Wie konfiguriere ich den Service, um meine Webserver zu durchsuchen?
11. Funktioniert Web Application Security auch in Verbindung mit einer Firewall?
12. Durchsucht Web Application Security meine ganze Domain oder nur einen Teil der Website?
13. Nach welchen Schwachstellen sucht Web Application Security?
14. Wie lange dauert eine Suche?
15. Wie beeinträchtigt die Suche meine Webserver?
16. Welche Arten von Schwachstellenberichten gibt es?
17. Erhalten Benutzer eine E-Mail-Benachrichtigung über die Ergebnisse der Sicherheitsprüfung?
18. In welchem Dateiformat werden die Berichte erstellt?
19. Wie wird der Schweregrad in den Berichten bewertet?
20. Welchen CVSS-Einstufungen entsprechen die Schweregrade Kritisch / Schwerwiegend / Mittel?
21. Was bedeuten die unterschiedlichen Schweregrade im Bericht der Schwachstellenbewertung?

Allgemeines

1. **Frage:** Was ist die Trend Micro Web Application Security Lösung?

Antwort: Mit Hilfe der Trend Micro Web Application Security Lösung können Unternehmen ihre Websites schützen, bevor Systeme infiziert werden. Die Lösung sucht rund um die Uhr nach Anzeichen eines Hackerangriffs, um Wiederherstellungsmaßnahmen einzuleiten. Diese werden über einen gehosteten Service durchgeführt, der die folgenden Funktionen bietet:



Web Application Security reduziert Zeitaufwand, Risiko und Kosten für den Schutz einer Website erheblich, da die Lösung auf Ihren Websites automatisch Webanwendungen, Netzwerke und Host-Betriebssysteme nach Sicherheitslücken und Schwachstellen durchsucht und über einen gehosteten Service qualifizierte Berichte zur Behebung der Risiken erstellt. Um E-Commerce-Domains auszuzeichnen, kann zusätzlich das Trend Micro SecureSite Vertrauenssiegel angezeigt werden, das die Sicherheit Ihrer Website bestätigt.

Der Überwachungsservice von Web Application Security ist im permanenten Austausch mit dem Trend Micro Smart Protection Network und sucht nach Anhaltspunkten für eine Infektion Ihrer Website. Ist Ihre Website infiziert, werden Sie sofort auf das Vorhandensein bössartigen Inhalts aufmerksam gemacht.

Demnächst bietet der Advanced-Service auch detaillierte Berichte zur Einhaltung von Richtlinien (z. B. PCI, SOX und HIPAA) mit Angaben, ob sich Verstöße ereignet haben und welche Maßnahmen zur Behebung durchgeführt werden sollten.

Trend Micro™ – Häufig gestellte Fragen (FAQ)

Trend Micro Web Application Security

Service-Aktivitäten - Version 1.0	Standard	Advanced Demnächst
Suche nach Schwachstellen in Webanwendungen	X	X
Suche nach Schwachstellen auf Hosts	X	X
SecureSite Vertrauenssiegel-Service	X	X
Infiltrierungswarmmeldungen	X	X
Suche nach Anforderung*	X	X
Berichte	X	X
Suche und Berichte zur Einhaltung von Richtlinien (u. a. PCI, SOX, HIPAA)		X

*5 Suchläufe pro Jahr beim Standard-Service. Zusätzliche Suchläufe bei Bedarf sind als Add-on verfügbar.

2. **Frage: Warum muss ich meine Websites vor Angriffen schützen?**

Antwort: Websites sind die offene Tür in Ihr Unternehmen. Sie sind Ihr Aushängeschild, und Sie erhöhen damit Ihre Umsatzchancen. Viele Websites haben aber Schwachstellen, von denen das Unternehmen zwar nichts weiß, aber durch die ihre Kunden und Daten trotzdem potenziellen Angriffen ausgesetzt sind. Dass diese Websites oft auch noch von Dritten entwickelt und gehostet werden, trägt nicht gerade zur Vereinfachung des Problems bei. Studien zeigen, dass viele Websites unzureichend geschützt sind:

- Über 79 % der Websites, auf denen sich bösartiger Code befindet, sind rechtmäßige Websites, die durch Hacker manipuliert wurden (ZDNet, April 2008)
- Von über 28.000 bekannten XSS-Schwachstellen auf namentlich erwähnten Websites wurden nur 5 % behoben (XSSed.com, August 2008)
- Über 40 % aller Internet-Bedrohungen traten auf seriösen Websites auf, über die unwissentlich Malware verbreitet wurde (TrendLabs, 2008)

3. **Frage: Wie können Malware oder Hacker meine Website und mein Unternehmen schädigen?**

Antwort: Hacker und Online-Kriminelle schlagen aus Sicherheitslücken im Internet Profit, indem sie vertrauliche Daten, wie z. B. Kreditkartennummern, entwenden. Täglich kommt es zu neuen Angriffen auf E-Commerce- und andere Websites. Für die meisten Unternehmen ist es extrem zeit- und ressourcenaufwändig, sich mit den zahlreichen Bedrohungen, wie z. B. Web-2.0-Angriffen, SQL-Injections und anderen websiteübergreifenden Schwachstellen, auseinanderzusetzen. Der Schutz vertraulicher Daten liegt jedoch in der Verantwortung des Unternehmens, unabhängig davon, ob es sich um Daten von Mitarbeitern, Kunden oder Unternehmenspartnern handelt. Die Anstrengungen zum Schutz der Website lenken vom Wesentlichen, dem Wachstum des Unternehmens, ab – ein Teufelskreis. Das Vertrauen Ihrer Kunden und Partner zu verlieren, würde dem Ruf Ihres Unternehmens schaden und umsatzsteigernde Aktivitäten gefährden. Viele Millionen Kunden schrecken aus Furcht vor Betrug und Identitätsmissbrauch davor zurück, ihre Kreditkarte im Internet zu verwenden.

4. **Frage: Woher weiß ich, ob Web Application Security die richtige Lösung für mein Unternehmen ist?**

Antwort: Web Application Security ist für Sie die richtige Lösung, wenn Sie:

- Zeitaufwand, Risiko und Kosten für das Erkennen und Beheben von Sicherheitslücken auf Ihren Websites reduzieren wollen
- Eine einfache und kostengünstige Möglichkeit suchen, den Sicherheitsstatus Ihrer Websites einzuschätzen und zu überwachen

Trend Micro™ – Häufig gestellte Fragen (FAQ)

Trend Micro Web Application Security

- Unterstützung von einem erfahrenen Sicherheitsexperten benötigen, um neuen und bestehenden Kunden, Partnern und Mitarbeitern ein sichereres Online-Erlebnis zu ermöglichen.
- Starke Datenschutzverfahren entwickeln wollen und die Sicherheit Ihrer Webanwendungen und -systeme sicherstellen.
- Potenzielle Sicherheitsprobleme lösen wollen, bevor sie Ihrem Unternehmen schaden.
- Kosten für den Erwerb und die Wartung mehrerer Produkte vermeiden wollen.
- Installation und Verteilung durch Bereitstellung eines entsprechenden Service vereinfachen wollen, so dass keine zusätzliche Hardware oder Software nötig ist.

5. **Frage:** Was bedeutet das SecureSite Vertrauenssiegel?

Antwort: Das SecureSite Vertrauenssiegel verdeutlicht als Gütesiegel eines unabhängigen Dritten Ihren E-Commerce-Kunden, dass Sie geeignete Maßnahmen zum Schutz ihrer Daten ergriffen haben. Es ist ein optional verfügbarer Service, der Websites täglich nach Schwachstellen, gefährlichen Inhalten und Links durchsucht, die PCs und vertrauliche Daten von Kunden dem Missbrauch aussetzen. Websites, die die Sicherheitsrichtlinien erfüllen, erhalten das neue Trend Micro SecureSite Vertrauenssiegel, woran Internet-Nutzer erkennen, dass der Betreiber der Website dem Thema Sicherheit ausreichend Bedeutung beimisst. Web Application Security Kunden, die ein anderes Suchintervall als "täglich" auswählen, können das SecureSite Vertrauenssiegel nicht auf ihrer Website anzeigen.

6. **Frage:** Wie kann Trend Micro feststellen, ob meine Website angegriffen wurde?

Antwort: Das Trend Micro Smart Protection Network ist eine webbasierte Content-Security-Infrastruktur der nächsten Generation, die ein weltumspannendes Netz aus Sensoren mit laufend aktualisierten und korrelierten Bedrohungsdatenbanken verbindet. Die Datenbanken bieten umfassenden Schutz vor allen Arten von Bedrohungen – von bösartigen Dateien, Spam, Phishing und Internet-Bedrohungen bis hin zu Denial-of-Service-Angriffen, Sicherheitslücken im Internet und sogar Datenverlust. Web Application Security überwacht permanent das Trend Micro Smart Protection Network, das nach Anhaltspunkten für eine Infektion Ihrer Website sucht. Ist eine Ihrer Websites infiziert, werden Sie sofort per E-Mail gewarnt, dass bösartige Inhalte vorhanden sind. Sie können dann die notwendigen Gegenmaßnahmen ergreifen, um weiteren Schaden an Ihren Unternehmenswerten und Ihrem Ruf zu verhindern. Der Überwachungsprozess erfordert keine dedizierte Suche auf Ihren tatsächlichen Websites, sondern nutzt das Echtzeitwissen des Smart Protection Network über Bedrohungen im Internet. Wenn Ihre Website einen Vertrauens- oder Sicherheitsstatus beibehält, sendet Trend Micro Ihnen regelmäßig eine E-Mail zur Bestätigung dieses Status. Hieran erkennen Sie, dass wir stets für Ihre Sicherheit sorgen.

7. **Frage:** Kann ich Trend Micro Web Application Security testen?

Antwort: Ja. Der Web Application Security Service ist als Testversion verfügbar. Die Registrierungsseite für die Testversion finden Sie unter:

<http://de.trendmicro.com/de/solutions/enterprise/security-solutions/web-application-security/trial>

Um sich zu registrieren, ist die Angabe einer öffentlich zugänglichen Domain- oder Host-IP-Adresse und einer gültigen E-Mail-Adresse erforderlich. Durch die Auswahl von Datum und Uhrzeit können Sie den Zeitpunkt der Suche an Ihre Anforderungen anpassen. Sie erhalten eine E-Mail zur Bestätigung Ihrer Registrierung und werden aufgefordert, einen kleinen Textausschnitt auf Ihrer Website zu hinterlegen, der Sie als Eigentümer der betreffenden Domain ausweist. Nach Abschluss der Testsuche erhalten Sie eine E-Mail, sobald Ihr Schwachstellenbericht zum Download bereitsteht. Die Bestätigung enthält einen Link mit Konto- und Kennwortdaten für den Zugriff auf eine Zusammenfassung Ihrer Suchergebnisse und die Wiederherstellungsberichte (Hinweis: Produktionskunden erhalten Konto- und Kennwortdaten per Telefon übermittelt, um den Datenschutz sicherzustellen. Diese Berichte stehen Ihnen 30 Tage lang auf einem nicht öffentlichen, sicheren Webportal zur Ansicht zur Verfügung. In der Testversion wird nur eine Domain oder IP-Adresse nach

Trend Micro™ – Häufig gestellte Fragen (FAQ)

Trend Micro Web Application Security

Schwachstellen durchsucht. Die Vollversion des Service unterstützt Unternehmen jedoch bei der Überwachung von 16 oder mehr Domains.

Technisches

8. **Frage:** Wie funktioniert der Web Application Security Service?

Antwort: Da es sich bei der Schwachstellensuche von Web Application Security um einen gehosteten, webbasierten Service handelt, können Ihre Websites schnell und einfach ohne zusätzliche Hardware oder Software durchsucht und geschützt werden. Zusätzlich profitieren Sie bei der gehosteten und von Trend Micro verwalteten Sicherheit immer von der neuesten Technologie und dem besten Schutz.

- Nach Ihrer Anmeldung am Service durchsucht Web Application Security Ihre Website gemäß Ihrem Zeitplan nach Schwachstellen oder Sicherheitslücken.
- Nach der Suche ermittelt Web Application Security das Risiko und liefert Wiederherstellungsberichte, mit deren Hilfe Sie schnell und wirksam reagieren können, um Ihre Website sicherer zu machen.
- Die Berichte beschreiben den Sicherheitsstatus Ihrer Website einschließlich möglicher Schwachstellen, dem Schweregrad der entdeckten Risiken sowie Problemlösungsvorschlägen von Experten. Suchen können nach Anforderung durchgeführt werden, um zu überprüfen, ob die von Ihnen ergriffenen Wiederherstellungsmaßnahmen erfolgreich waren.
- Wenn Ihre Website unseren Sicherheitskriterien entspricht und Sie täglich eine Suche durchführen, berechtigt Sie dies zur Anzeige des SecureSite Vertrauenssiegels auf Ihrer Website. Hieran erkennen Online-Kunden, dass zusätzliche Schritte unternommen werden, um ihre Daten und ihre Privatsphäre zu schützen.
- Web Application Security überwacht rund um die Uhr das Trend Micro Smart Protection Network, um nach Anhaltspunkten für eine Bedrohung der Sicherheit Ihrer Website zu suchen. Sobald bösartiger Inhalt auf Ihrer Website entdeckt wird, werden Sie per E-Mail gewarnt.

9. **Frage:** Welche Arten von Website-Anwendungskomponenten durchsucht Web Application Security?

Antwort:

Sucht in	Beispiele	Schützt vor
Anwendungsschicht	<u>Webinfrastruktur:</u> Apache, Apache Tomcat, Microsoft Internet Explorer, Mozilla FireFox, Microsoft IIS, FTP, BEA Weblogic, Adobe ColdFusion, SSH, TELNET und Warenkörbe <u>Web 2.0:</u> JavaScript, AJAX, Adobe-Flash-Anwendungen <u>Webseiten:</u> Formulare und Inhalte auf der Website	<ul style="list-style-type: none">• Infektion von Websites durch Ausnutzung von 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	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

Trend Micro™ – Häufig gestellte Fragen (FAQ)

Trend Micro Web Application Security

Netzwerkssysteme	Cisco Firewalls, IPSec, PPTP, Network File System (NFS), DHCP, DNS, LDAP, SNMP	<ul style="list-style-type: none"> • Probleme bei 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	<ul style="list-style-type: none"> • Zu- oder Angriff auf ein Betriebssystem durch Richtlinienverstöße, wie z. B. vorhersehbare Kennwörter, Dateiberechtigungen oder unangemessener Kontozugriff

10. **Frage:** Wie konfiguriere ich den Service, um meine Webserver zu durchsuchen?

Antwort: Von unserem Operations Team erhalten Sie ein Web Application Security Konfigurationsformular, auf dem Sie die Domains und/oder IP-Adressen angeben, die auf Schwachstellen und bösartige Inhalte durchsucht und überwacht werden sollen.

11. **Frage:** Funktioniert Web Application Security auch zusammen mit einer Firewall?

Antwort: Ja. Möglicherweise müssen Sie die IP-Adresse des Trend Micro Suchservers zur Weißen Liste Ihrer Firewall oder Ihres IDS/IPS hinzufügen, um zu verhindern, dass die Suche versehentlich als bösartiger Angriff gesperrt wird.

12. **Frage:** Durchsucht Web Application Security meine gesamte Domain oder nur einen Teil der Website?

Antwort: Es werden alle Links zu Seiten der Website durchsucht, die noch zur betreffenden Domain gehören. Externe Links werden nicht berücksichtigt.

13. **Frage:** Nach welchen Schwachstellen sucht Web Application Security?

Antwort:

Ermöglicher von Betrug und Phishing	
Cross-Site-Scripting	Betrügt Benutzer: Die meisten Branchenexperten sind sich einig, dass Cross-Site-Scripting (XSS) auch weiterhin die häufigste Schwachstelle von Websites sein wird. Je nach Website kann XSS für Unternehmen und Kunden ein besonders hohes Risiko darstellen. Neue Angriffswege sind für hochwirksame Phishing-Angriffe und Internet-Würmer verantwortlich, gegen die herkömmliche Schutzmaßnahmen wirkungslos sind. Durch die Entwicklung neuester JavaScript-Malware als Schadteil ist es dringender als je zuvor, diese Schwachstelle zu entdecken und zu beheben.
Datenlecks	
Entwendung von Daten	Stiehlt proprietäre Daten: Datenlecks treten auf, wenn eine Website irrtümlich vertrauliche Daten, wie z. B. Entwicklerkommentare, Benutzerdaten, interne IP-Adressen, Quellcode, Überarbeitungsnummern und Fehlermeldungen/-codes, preisgibt oder entsprechend manipuliert wurde, und so einem Angreifer Hilfestellung leistet.

Trend Micro™ – Häufig gestellte Fragen (FAQ)

Trend Micro Web Application Security

Vorhersehbarer Link	<p>Verwendet Google Hacks: Die einzige Möglichkeit zum Schutz der darin enthaltenen, vertraulichen Daten ist in der Regel die Vorhersehbarkeit des Links. Automatische Scanner können mittlerweile sehr einfach Tausende mutmaßlicher Links erzeugen, um diese Dateien aufzudecken. Außerdem setzen Angreifer mit Hilfe des so genannten „Google Hacking“ Suchmaschinen ein, um vertrauliche Daten über vergessene Links auf einer Website aufzudecken.</p> <p>Findet versteckte Seiten: Mit der Zeit enthält eine Website viele Seiten, die nicht mehr verlinkt sind und nicht mehr gewartet werden. Dazu zählen häufig Webseiten mit Zahlungsprotokollen, Software-Backups, zukünftigen Pressemitteilungen, Fehlermeldungen oder Quellcode.</p>
SQL-Injection	<p>Entwendet Datenbankinhalte: Einige der größten Betrugsfälle durch Kreditkarten- und Identitätsmissbrauch machten sich SQL-Injection zunutze. Die heutigen Website-Datenbanken am Backend speichern hochvertrauliche Daten. Dies macht sie naturgemäß zu einem attraktiven Ziel für bösartige Hacker. Namen, Adressen, Telefonnummern, Kennwörter, Geburtsdaten, geistiges Eigentum, Geschäftsgeheimnisse, Kodierungsschlüssel und meist noch viel mehr könnten von Diebstahl bedroht sein. Mit einigen gut platzierten Anführungszeichen, Strichpunkten und SQL-Befehlen können ganze Datenbanken in falsche Hände gelangen.</p>
Verzeichnisindizierung	<p>Findet proprietäre Seiten: Die meisten Webserver verfügen über diese Funktion, die bei Fehlen von Dateinamen und Indexdatei (z.B. index.htm) den Inhalt eines Verzeichnisses listet. Verzeichnislisten können unter Umständen vertrauliche Daten, die nicht für die Öffentlichkeit bestimmt sind, wie vorab veröffentlichte Webseiten, Protokolldateien, temporäre Dateien, Sicherungskopien usw., offenlegen.</p>
Xpath-Injection	<p>Extrahiert vertrauliche Daten: Ähnlich wie SQL-Injection nutzt auch diese Angriffstechnik Schwachstellen auf Websites aus, die XPath-Abfragen über Benutzereingaben erstellen. Wenn ein Angreifer in der Lage ist, eine XPath-Abfrage zu ändern, kann er möglicherweise auch vertrauliche Dateien aus einem XML-Dokument ermitteln, auf das er sonst nicht zugreifen könnte.</p>
Unbefugte Nutzung	
Unzureichende Authentifizierung	<p>Ermöglicht betrügerischen Zugriff: Diese Sicherheitslücke findet sich typischerweise in der Anwendungslogik einer Software. Bei erfolgreicher Ausnutzung können Angreifer ohne Autorisierung auf geschützte Bereiche einer Website zugreifen. So kann sich ein Angreifer beispielsweise als normaler Benutzer anmelden und für einen anderen Benutzer im System ausgeben.</p>
Funktionalitätsmissbrauch	<p>Verwendet Website-Funktionen gegen den Benutzer/Eigentümer: Die Web Application Security Consortium Threat Classification definiert den Funktionsmissbrauch als „eine Angriffsmethode, die die Eigenschaften und Funktionen der Website selbst verwendet, um Zugangskontrollen auszuschalten, zu überlisten oder zu umgehen. Einige Funktionen einer Website, möglicherweise sogar Sicherheitsfunktionen, können missbraucht werden, um unerwartetes Verhalten zu verursachen. Wenn eine Funktion anfällig für Missbrauch ist, kann ein Angreifer möglicherweise andere Benutzer belästigen oder sogar das gesamte System betrügen.“</p>
Pufferüberlauf	<p>Übernimmt die Steuerung von Servern: Nutzt Schwachstellen auf Websites aus, um die vollständige Kontrolle über einen Server zu übernehmen und bösartige Aktivitäten durchzuführen.</p>

14. Frage: Wie lange dauert eine Suche?

Antwort: Die Dauer einer Suche hängt von der Größe Ihrer Website, der Anzahl der Formulare und der entdeckten Schwachstellen ab. In der Regel kann eine einzelne Domain oder IP-Adresse in weniger als 15 Minuten durchsucht werden. Beim ersten Suchzyklus überwacht Trend Micro die Suchdauer für Ihre Domains und Hosts, damit Sie zukünftige Suchen effizienter planen können.

Trend Micro™ – Häufig gestellte Fragen (FAQ)

Trend Micro Web Application Security

15. **Frage:** Beeinträchtigen die Suchläufe meine Webserver?

Antwort: Web Application Security wendet keine Suchtechniken an, von denen bekannt ist, dass sie den Netzwerkverkehr stören. Allerdings kann kein Netzwerk-Scanner gewährleisten, dass es durch die Suche zu keinen Beeinträchtigungen oder Störungen aller Systeme kommen kann. Wenn der Service beispielsweise Webanwendungen auf XSS- oder SQL-Injection-Schwachstellen überprüft, muss er jede Seite der Ziel-Website verarbeiten und die Formulare zur Analyse der Serverreaktion einsenden. Bei Fragen können Sie sich gerne unter wfss_support@trendmicro.com an Trend Micro wenden.

16. **Frage:** Welche Arten von Schwachstellenberichten gibt es?

Antwort: Web Application Security bietet sowohl eine Zusammenfassung als auch einen Wiederherstellungsbericht.

- **Zusammenfassung:** Eine Zusammenfassung der Ergebnisse der Sicherheitsprüfung mit Übersichten und Tabellen, die den Zustand Ihres Netzwerks und Ihrer Webserver verdeutlichen, wie beispielsweise vorhandene Schwachstellen nach Schweregrad und Kategorie.
- **Wiederherstellungsbericht:** Eine detaillierte Auswertung mit Kennzeichnung der Sicherheitsrisiken, die Ihre kritischen Webvorgänge und -werte beeinträchtigen könnten. Dieser Bericht enthält die Anzahl der Risiken sowie einen Gesamtrisikoindex für jedes System. Dadurch können Sie Ihren Wiederherstellungsmaßnahmen Prioritäten zuweisen. Für jeden Host und jede Sicherheitslücke werden ein umfassender Plan und eine Reihe von Tipps zur Wiederherstellung inklusive einer Einschätzung der erforderlichen Zeitdauer erstellt.

17. **Frage:** Können Benutzer eine E-Mail-Benachrichtigung zu den Ergebnissen der Sicherheitsprüfung erhalten?

Antwort: Ja. Web Application Security benachrichtigt Sie nach Abschluss jeder Suche und bei der Bereitstellung der Berichte im Webportal. Wenn das Trend Micro Smart Protection Network gehostete Inhalte auf Ihrer Website als bösartig identifiziert, erhalten Sie zusätzlich eine Warnmeldung mit detaillierten Informationen über die infizierte Website und die entdeckte Malware.

18. **Frage:** Welche Dateiformate kann Web Application Security zur Erstellung von Berichten verwenden?

Antwort: Berichte werden ausschließlich im PDF-Format in unserem sicheren Webportal bereitgestellt und sind über Ihr Konto abrufbar.

19. **Frage:** Wie wird der Schweregrad in den Berichten bewertet?

Antwort: Unsere Bewertungen basieren auf dem CVSS-Bewertungssystem (Common Vulnerability Scoring System) und weisen jeder Sicherheitslücke einen Wert von 1 bis 10 zu (siehe <http://nvd.nist.gov/cvss.cfm>.) Außerdem wird unsere 1-10-Bewertungsskala auf die PCI-Skala abgebildet, damit wir PCI-Berichte erstellen können. PCI-Berichte basieren auf einem eigenen Bewertungssystem für Schweregrade und Kategorien, die von unserem System abweichen können. So werden alle Denial-of-Service-Angriffe mit 3, alle Würmer mit 5 usw. eingestuft.

20. **Frage:** Welchen CVSS-Einstufungen entsprechen die Schweregrade Kritisch / Schwerwiegend / Mittel?

Antwort:

- **Kritisch:** Sicherheitslücke in einem leicht zugänglichen System, das wenig oder keine Authentifizierung erfordert und es ermöglicht, auf vertrauliche Daten zuzugreifen, Daten zu beschädigen/löschen oder das System auszuschalten. Bewertung zwischen 8 und 10 im CVSS-Bewertungssystem. Beispiele: Kein Kennwort für CIFS-Administratorkonto, anonyme Benutzer können auf die Windows Kennwortrichtlinie zugreifen.
- **Schwerwiegend:** Schwachstelle in einem System, das mit mäßiger Hacking-Erfahrung zugänglich ist, möglicherweise keine Authentifizierung erfordert und es ermöglicht, teilweise auf geschützte Daten oder auf das System zuzugreifen und Daten zu zerstören und/oder einzelne Systeme in einem Netzwerk zu deaktivieren. Bewertung zwischen 4 und 7 im CVSS-Bewertungssystem. Beispiele: Anonymer Schreibzugriff auf ein FTP-Verzeichnis, schwaches LAN-Manager-Hashing.
- **Mittel:** Schwachstelle in einem System, das lokalen Zugriff ermöglicht, Authentifizierung erfordert und es ermöglicht, nicht oder in geringem Umfang auf geschützte Daten zuzugreifen, keine Daten zu zerstören oder zu beschädigen und/oder keine Systeme abzuschalten. Bewertung zwischen 1 und 3 im CVSS-Bewertungssystem. Beispiele: Leicht zu erratende oder Standardnamen für SNMP-Communities: public, OpenSSL PRNG Internal State Discovery Vulnerability.

21. **Frage:** Was bedeuten die unterschiedlichen Schweregrade im Bericht der Schwachstellenbewertung?

Antwort: Kritische Schwachstellen sind solche, die remote ausgenutzt werden können, Root- oder Administratorzugriff erlauben oder einen aktiven „In-the-Wild“-Wurm oder -Virus beinhalten. Schwerwiegende Schwachstellen können nur lokal ausgenutzt werden und ermöglichen keinen Root-Zugriff. Auch DoS-Angriffe zählen zu dieser Kategorie. Über mittlere Sicherheitslücken können möglicherweise vertrauliche Daten ausspioniert werden. Diese Kategorie kann in Verbindung mit anderen Schwachstellen zur Vorbereitung eines Angriffs verwendet werden.