

So schützen Sie sich gegen neue Sicherheits- risiken aus dem Internet

*Das mehrstufige Verfahren zur
Vervollständigung
herkömmlicher
Schutzmaßnahmen*

Websense Deutschland GmbH
Vertriebsniederlassung
Leopoldstrasse 244
80807 München
Deutschland

Telefon: +49 89 24445 4005
Fax: +49 89 24445 1200
www.websense.de

Zusammenfassung

Unternehmen und Institutionen müssen Schutzmaßnahmen für die von ihnen eingesetzte IT-Infrastruktur ergreifen. Die IT-Systeme, die durch Mitarbeiter genutzt werden, haben sich im Laufe der Zeit erheblich gewandelt. Gerade das Internet bietet ein breites Angebot an interessanten Inhalten und neuen Anwendungen. In Folge dieser Entwicklung sind Unternehmen heute mit einer größeren Zahl von Sicherheitsrisiken als jemals zuvor konfrontiert. Angriffe aus dem Internet, wie sie in jüngster Zeit aufgetreten sind, weisen deutlich auf die Unzulänglichkeiten der Mehrzahl aller derzeit eingesetzten IT-Security-Lösungen hin. Firewallsysteme am Gateway, die lediglich mit einer Antivirensoftware kombiniert werden, bieten keinen ausreichenden Schutz gegen komplexe, bössartige Programme, die eine Bedrohung für die unternehmenseigene IT-Infrastruktur darstellen. Hier werden von IT-Abteilungen passende Lösungen gefordert.

Das vorliegende Whitepaper untersucht einige neuere Vorfälle und erläutert, weshalb Software von Websense hier einen wirkungsvollen Schutz bietet. Da die Filterfunktionen von Websense an mehreren Punkten im Netzwerk, am Gateway und auf Desktopebene wirken, können Lösungen von Websense einen vollständigen Schutz vor den im vorliegenden Dokument beschriebenen neuen, zuvor unbekanntenen Gefahrenquellen bieten.

Inhalt

Zusammenfassende Darstellung	1
Hintergrundinformationen.....	1
Das Problem	1
Aktuelle Beispiele für Gefahrenherde	2
Die Websense-Story	3
Chronologie	3
So schützt Websense vor Angriffen aus dem Internet.....	3
Fazit	3
Über Websense Inc.	3

Zusammenfassende Darstellung

Angriffe aus dem Internet, wie sie in jüngster Zeit beobachtet wurden, sind ein deutlicher Beweis für die Unzulänglichkeiten der Mehrzahl aller derzeit eingesetzten Sicherheitslösungen. Firewallsysteme am Gateway, die lediglich mit einer Antivirensoftware kombiniert werden, bieten keinen ausreichenden Schutz gegen komplexe, bösartige Programme, die eine Bedrohung für IT-Systeme darstellen. Firewalls können lediglich erkennen, ob Daten mit dem Internet ausgetauscht werden. Sie sind jedoch meist nicht in der Lage, den Datenverkehr zu überwachen und gezielt bestimmte Inhalte zu filtern. Andererseits wirken Antiviren-Lösungen erst nachträglich und nicht vorbeugend; ihr Schutz richtet sich nur gegen ganz bestimmte Risiken und selbst dieser begrenzte Schutz greift erst, nachdem der Angriff bereits erfolgt ist. Unternehmen benötigen deshalb Lösungen, die Firewall- und Antivirensoftware um eine Schutzschicht auf Inhaltsebene ergänzen. Das vorliegende Dokument zeigt, dass mit Software von Websense ein vollständiger Schutz gegen neue, kombinierte Gefahren gewährleistet werden kann.

Hintergrundinformationen

Das Problem

Eine der wichtigsten Aufgaben des IT-Managers ist die Bereitstellung offener, unternehmensweit nutzbarer Netzwerkumgebungen. Gleichzeitig liegt es jedoch in deren Verantwortung, das Unternehmen vor finanziellen Verlusten und Rechtshafungsrisiken zu schützen, die als Folge von Sicherheitslücken entstehen könnten. Viele Unternehmen begegnen diesem Problem mit Hilfe einer Kombination aus Sicherheitsprodukten und -Dienstleistungen verschiedener Anbieter. Die hierbei verwendeten Technologien, also z.B.

Antivirensoftware, Firewalls und Intrusion Detection Systeme leisten meist ausgezeichnete Arbeit innerhalb ihres jeweiligen Aufgabenfeldes, können aber keinen ausreichenden Schutz gegen entsprechend ausgerichtete Malware wie Code Red und Nimda bieten, die laut einer Studie des Unternehmens Computer Economics weltweit einen Schaden verursacht, der auf 3 Milliarden US-Dollar geschätzt wird.

In den vergangenen Monaten ist das Gefahrenpotenzial für den Internetnutzer weiter angestiegen – in vielen Fällen erfolgten Angriffe aus dem Internet mit dem Ziel, schädliche Software in lokalen Netzwerke einzuschleusen. In einigen Fällen wurden insbesondere Schwächen und Fehlfunktionen von Webbrowsern ausgenutzt – z.B. bei den Internetangriffen im Juni und Juli 2004. Hier zeigt sich deutlich, dass Hacker inzwischen hoch entwickelte Kombinationen verschiedener Methoden (= "Blended Threats") verwenden, um Benutzer mittels nachgeahmter Websites zu täuschen bzw. dass es sehr einfach ist, mit Hilfe von Malicious Code Benutzerdaten, Kennwörter und andere vertrauliche Informationen auszuspähen.

Blended Threats

Nimda und Code Red sind zwei Beispiele für schädliche Software mit komplexen Infektions- und Verbreitungsmechanismen, so genannte „Blended Threats“. Solche Programme bedienen sich derselben Verbreitungswege wie gewöhnliche Viren und Würmer. Gleichzeitig nutzen sie aber auch die Sicherheitslücken weit verbreiteter Anwendungsprogramme und Betriebssysteme, um sich zu verbreiten oder Daten zu manipulieren. Viren bestehen meist aus einem Skript oder Makro bzw. sind in eine ausführbare Datei eingebaut. Würmer verbreiten sich häufig über den Hauptspeicher oder von Festplatte zu Festplatte. Die Infektion durch Blended Threats kann wie bei einem E-Mail-Virus über massenhaft verschickte E-Mail-Attachments erfolgen aber auch gezielt nach Softwareversionen suchen, deren Sicherheitslücken nicht durch ein Update geschlossen worden sind und sich so Zugang zum Betriebssystem oder einer Anwendung verschaffen. Gelangt ein solches Blended Threat auf einen Desktop- oder Server-PC, kann es dort Dateien zerstören oder verändern. Aber Blended Threats können noch weitere Gefahren beinhalten, wie z.B. vom Programmierer integrierte geheime Zugänge, die so genannten Backdoors. Auch scheinbar harmlose Programme, die man Trojaner nennt, und „Zombies“, also kleine Programme, die bei einer späteren Aktivierung gemeinsam mit vielen anderen infizierten Systemen für so genannte Denial-of-Service-Angriffe eingesetzt werden und einen bestimmten Server mit Datenanforderungen überlasten sollen, können auf diesem Wege von Hackern automatisiert in fremde Systeme eingeschleust werden.

InformationWeek vom 20.4.2002

Hacker nutzen die Schwächen des Webbrowsers, um in die Seiten vertrauenswürdiger Websites Datenstrukturen einzuschleusen, die dann beispielsweise die Kreditkarteninformationen des Benutzers ermitteln. Der Nutzer wähnt sich auf einer vertrauenswürdigen Website, z.B. im Online-Banking-Formular seiner Bank oder auf der Bestellseite eines Online-Shops. In Wirklichkeit handelt es sich bei der angezeigten Seite aber um eine von Hackern geschaffene, täuschend echt wirkende Fälschung.

Beinahe täglich werden neue Vorfälle bekannt – Web-Attacken, Spyware, Malicious Mobile Code oder Phishing-Angriffe. Weltweit entstand so im Jahr 2003 ein geschätzter Schaden von 12,5 Milliarden US-Dollar.¹ Für Unternehmen sind der Zeitpunkt des Auftretens, der Ausgangspunkt bzw. die genauen Umstände einer solchen Gefahr nicht vorhersehbar. Entscheidend für die Bewältigung ist die rechtzeitige Planung von Schutzmaßnahmen des Unternehmens für den Fall neuer, bis zu diesem Zeitpunkt unbekannter und zunehmend gefährlicher Risiken.

„Die Vorbereitung auf einen solchen Vorfall erfordert eine sicherheitstechnische Architektur, die bekannte und unbekannte Gefahrenquellen automatisch erkennen und unterdrücken kann. Die heute vorherrschenden [Antiviren-]Technologien verhindern Infektionen mit Filterfunktionen, die anhand von Signaturen arbeiten. Dieses Verfahren funktioniert allerdings nur, wenn die Sicherheitslücken bzw. die Exploit-Software bekannt ist. Bedenkt man die sinkenden Zeitabstände zwischen dem Bekanntwerden von Sicherheitslücken und dem Auftauchen von Exploits, ist ein solches Verfahren unzureichend. Ziel sollte eine ausreichende Zahl an Sicherheitsschichten sein, damit eine Sicherheitslücke einer einzelnen Schicht nicht den gesamten Geschäftsbetrieb eines Unternehmens gefährdet.

Eric Litt, Chief Information Security Officer, General Motors in der Zeitschrift Computerworld vom 12.7.2004

Aktuelle Beispiele für Gefahrenherde

Im Juni und Juli 2004 trat eine neue Form von Malware in Erscheinung, die unter dem Namen *JS/Scob-A* (bzw. *Download.Ject* und *Toofer*) Schlagzeilen machte. Bei diesem Vorfall wurde erstmals das World Wide Web selbst als Transportweg für Malicious Code genutzt.

Von Hackern veränderte Websites haben dabei ahnungslose Surfer mit Code infiziert, was nur durch Ausnutzung von Sicherheitslücken im Microsoft Internet Explorer und in bestimmten Webservern möglich war.

Beim Aufruf einer infizierten Seite wurde der Browser des Benutzers auf eine russische Website umgeleitet, die im Hintergrund eine Zugangssoftware (Backdoor) und ein Keylogging-Programm installierte. Das dabei installierte Programm wartete still im Hintergrund, bis es den Aufruf ganz bestimmter URLs (z.B. der einer Online-Bank) registrierte. Erst dann hat sich das Keylogging-Programm aktiviert. Vertrauliche Daten wie Benutzernamen, Kennwörter und Kontonummern wurden direkt an den Host-Computer der Hacker in Russland übermittelt. Anders als andere Angriffe in der jüngeren Vergangenheit, bei denen Malware in Folge einer Benutzerhandlung installiert wurden – z.B. durch Öffnen einer E-Mail oder Website (eine Methode, die als „Phishing“ bekannt ist), war hier keine Mitwirkung durch den Benutzer erforderlich.

Internetprovider und Strafverfolgungsbehörden haben in Zusammenarbeit mit Microsoft den russischen Webserver ausfindig gemacht und am 24.6.2004 stillgelegt. Obwohl die ausländische Website, über die *JS/Scob-A* verbreitet wurde, nun inaktiv ist, sollten IT-Administratoren mit Nachahmern dieser Methode rechnen.

„Die Sicherheitslage ändert sich täglich – Hacker setzen in ihrem Malicious Code immer ausgefeiltere Techniken ein, um in Unternehmensnetzwerke einzudringen und konventionelle Sicherheitsvorkehrungen wie Firewalls und Antiviren-Software zu umgehen.“ „In letzter Zeit erscheinen insbesondere Spyware, Instant Messaging und P2P als

¹ Quelle: InformationWeek vom 5.7.2004.

sehr verlockende Zugangswege für Computerkriminelle. Wegen des wesentlich höheren Risikos sollte man die Öffentlichkeit nicht nur auf diese Gefahren aufmerksam machen sondern auch Maßnahmen und Wege aufzeigen, um diese zu begrenzen.“

Lawrence Orans, Principal Analyst, Gartner Research

Die Websense-Story

Besitzer der Websense Enterprise® Security PG™-Software haben bereits frühzeitig einen verbesserten Schutz gegen den kürzlich in Erscheinung getretenen Trojaner *JS/Scob-A* (der auch unter den Namen *Download.Ject* und *Toofer bekannt ist*) erhalten. Technologie von Websense bewahrte Kunden dabei vor einer Infektion, bis der kritische Zeitabschnitt bis zum Erscheinen von geeigneten Antiviren-Signaturen überwunden war.

Chronologie

Websense wurde auf die von *JS/Scob-A* ausgehende Gefahr am Morgen des 24.6.2004 aufmerksam, als The Internet Storm Center (SANS) einen Bericht veröffentlichte, der auf einen im WWW kursierenden neuartigen Trojaner hinwies. Zur selben Zeit erreichte Websense eine Kundenanfrage, bei der es um die Aufklärung mysteriöser Datenübertragungen an eine Website in Russland ging. Noch am selben Tag ermittelten Websense Security Labs die Ursache des Vorfalls und nahm die russische Website in die Liste der gesperrten Sites von Security-PG auf.

Seit 25.6. suchen die Data Mining-Routinen bei Websense gezielt auch nach Websites, die mit dem neuen Malicious Code infiziert sind. Websense hatte kurze Zeit später bereits etwa 130 Websites gefunden, deren zusammen mehr als 10.000 URLs allesamt befallen waren. Die Datenbank aller Websense-Produkte wurde mit dem nächtlichen Update-Download um die betroffenen Webseiten ergänzt.

Am 28.6. machte Websense IT-Fachleuten in aller Welt Daten zu den betroffenen Browsern und Servern zugänglich. Aus den bereitgestellten Statistiken gingen auch die von Websense bis zu diesem Zeitpunkt ermittelten mehr als 130 eigenständigen Domains hervor. Die Websites liefen unter IIS 5.0 mit SSL, wobei sowohl über HTTP als auch über HTTPS zugängliche URLs betroffen waren. Die zugehörigen IP-Adressen stammten von Servern in den USA, Australien, Neuseeland, Kanada, Japan, Spanien, Großbritannien und Norwegen.

Am 29.6. haben weitere Analysen und Recherchen einen weiteren neuen Exploit ermittelt, der inzwischen unter dem Namen *IMBIG.Trojan* bekannt ist und der Benutzer ebenfalls über Websites infiziert. Dieser Exploit nutzt andere Sicherheitslücken im Internet Explorer sowie ein BHO (Browser Help Object), das Tastatureingaben aufzeichnet und an eine externe Website weiterleitet. Die Mitarbeiter von Websense stießen auf eine befallene Website und konnten den Programmcode des Trojaners rekonstruieren. Dabei stellte sich heraus, dass das Programm auf eine andere Website verweist, von der ein Teil des schädlichen Codes empfangen wird. Bei dieser neuen Version wurden zwei Anwendungen miteinander verknüpft. Websense hat die tägliche Updatedatei der Datenbank seiner Produkte um die hiervon betroffenen Webseiten ergänzt und alle ermittelten Informationen der IT-Security-Community zugänglich gemacht.

Tabella 1. Ereignisse im Überblick

Tag	Ereignis
24.6.	SANS veröffentlich Report zu neuem Trojaner. Websense-Kunde bittet um Hilfe bei der Untersuchung ungewöhnlicher Netzwerkdaten. Websense Security Lab nimmt russische Website in die Security-PG-Liste auf.
25.6.	Websense-Datamining-Verfahren um entsprechende Website-Suchfunktion erweitert; es werden 130 infizierte Sites ermittelt. Alle betroffenen Sites und Webseiten (10,000 URLs) werden in die Security-PG-Liste aufgenommen.
28.6.	Websense informiert Sicherheitsfachleute. Noch immer sind 130 eigenständige Domains befallen.
29.6.	Websense wird auf einen weiteren neuen Exploit (IMBIG.Trojan) aufmerksam und kann dessen Programmcode aufzeichnen und rekonstruieren. Websense aktualisiert seine Produkte; infizierte Sites werden blockiert. Websense informiert Sicherheitsfachkreise.
5.7. 6.7.	Antiviren-Signaturen für JS/Scob-A und IMBIG.Trojan werden verfügbar gemacht bzw. veröffentlicht.

„Ich bin davon überzeugt, dass diese spezielle Art von Malware eine enorme Gefahr für Online-Finanzdienstleister darstellt. Wie bereits die starke Zunahme an Ad- bzw. Spyware zeigt, ist die Installation von ausführbaren Programmen auf Desktop-PCs viel zu einfach. Der Einsatz von BHO macht diese Art des Datendiebstahls besonders heimtückisch.“

Tom Liston, SANS-Forscher nach der Analyse des Vorfalls in der Ausgabe vom 29.6.2004 von eWeek.com

Viele Anbieter von Antivirensoftware benötigten mehrere Tage, um geeignete Signaturen zu erstellen und verfügbar zu machen. Während dieses Zeitraums waren Websense-Kunden geschützt, obwohl auch ihnen noch keine entsprechenden Virussignaturen zur Verfügung standen.

Software von Websense setzt an drei unterschiedlichen Punkten an, um die Einhaltung von Nutzungsrichtlinien sicherzustellen: im Netzwerk, am Gateway und auf dem Desktop. Dieses mehrschichtige Sicherheitskonzept bietet auch Schutz vor neuartigen Bedrohungen. Security-PG verhindert einen Zugriff der Mitarbeiter auf Websites, die mit Mobile Malicious Code (MMC) infiziert sind und u.a. Trojaner verbreiten. Security-PG unterbindet die Übertragung von vertraulichen Daten an nicht freigegebene Server (z. B. den russischen Webserver). Security-PG beinhaltet u.a. den Zusatzdienst SiteWatcher™, der Unternehmen bei Infektion der Unternehmenswebsite durch MMC alarmiert.

„Die jüngsten Angriffe auf IT-Umgebungen werden zunehmend bösartiger und komplexer und konnten durch konventionelle Antivirensoftware nicht verhindert werden. Die Unsicherheitsfaktoren und das Schadenpotenzial für Netzwerke haben für IT-Security-Fachleute höchste Priorität. Mit Websense Enterprise Security-PG und dem Client Policy Manager können Käufer von Websense-Lösungen den Besuch infizierter Websites und damit eine unerkannte Infektion mit Malicious Mobile Code unterbinden und außerdem firmeneigene Computer und Netzwerke wirkungsvoll gegen Infektionen schützen.“

Dan Hubbard, Director of Security and Technology Research, Websense, Inc.

Zusätzlichen Schutz auf Desktopebene bietet der Websense® Client Policy Manager™ (CPM). Er stellt durch die Modi „Application Lockdown“ und „Network Lockdown“ sicher, dass MMC nicht in Computer eindringen kann, die durch Mitarbeiter genutzt werden. Bei aktiviertem Application Lockdown kann der Mitarbeiter nur solche Anwendungen ausführen, die durch das Unternehmen explizit freigegeben sind. Diese Funktion bietet einen sicheren Schutz gegen bösartige Trojaner und andere Gefahrenquellen aus dem Internet wie z.B. Spyware. Network Lockdown gewährleistet die Isolierung befallener Mitarbeiter-PCs. Im Netzwerk wird die Übertragung von Daten und der Schaden verursachenden Programme selbst unterbunden. Eine weitere Ausbreitung des Malicious Code nach dessen Eindringen ist ausgeschlossen.

Trotz der Abschottung durch Firewalls und Antiviren-Gateways stellen lokale Desktop-PCs noch immer eine Quelle für die Infektion mit Viren und Würmern dar. Dies gilt insbesondere für Mobilanwender, deren Computer unterwegs infiziert werden und die diese Infektion nach ihrer Rückkehr in das LAN einschleppen. Lokale Desktop-PCs stellen durch Trojaner, Spyware und schädliche Anwendungen, die aus dem Internet stammen, sowie durch nicht aktualisierte Betriebssysteme ebenfalls ein Risiko für das Netzwerk dar.

Network Magazine vom 1.7.2004

So schützt Websense vor Angriffen aus dem Internet

Websense gewährleistet die Einhaltung von Nutzungsrichtlinien an drei unterschiedlichen Punkten: im Netzwerk, am Gateway und auf dem Desktop. Dieses mehrschichtige Sicherheitskonzept bietet Schutz vor Angriffen aus dem Internet.

Die Websense-Datenbank bildet das Kernstück von Websense Enterprise®. Sie beinhaltet die branchenweit umfangreichste und aktuellste Liste häufig aufgerufener Websites. Die Websense-Datenbank ist nach Kategorien, Sites, Protokollen und Anwendungen geordnet und beinhaltet eine Liste der beliebtesten Websites, häufig verwendeter Internetprotokolle und PC-Anwendungen. Die Websense-Datenbank umfasst mehr als 8 Millionen Einträge zu Websites mit über 50 Milliarden Einzelseiten.

Neue Websites werden mit Hilfe proprietärer Softwareverfahren ermittelt, zu denen auch WebCatcher™ zählt. Bei der Kategoriezuweisung gelangen einzigartige Verfahren und Technologien aber auch Analysespezialisten zum Einsatz. Die Datenbank wird alle sieben Stunden aktualisiert, wobei eine tägliche Aktualisierung exakte Datenbestände durch Neueinträge, Änderungen und Löschungen gewährleistet.

Mit WebCatcher können Nutzer von Websense Enterprise bislang nicht kategorisierte URLs – also Websites, die nicht einer der über 90 Inhaltskategorien zugeordnet sind – zur Analyse an Websense übermitteln. Die einzigartige Technologie von Websense WebCatcher ermittelt unkategorisierte Websites anhand der Protokolldaten hunderter Websense-Kunden in aller Welt. Websites werden bewertet, einer Kategorie zugeteilt und in kürzester Zeit in die Websense-Datenbank aufgenommen. Da dies täglich geschieht, werden die Datenbestände kontinuierlich präzisiert und der Datenbankbestand ständig aktuell gehalten.

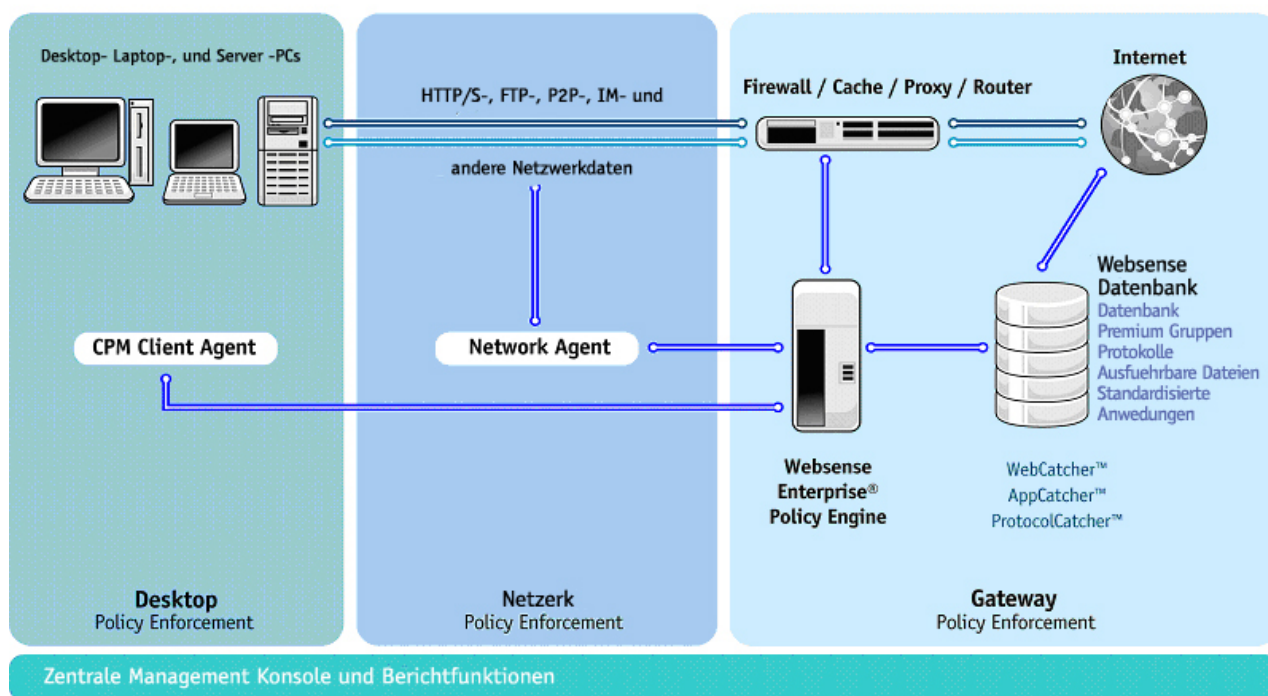


Abbildung 1. WebCatcher ermittelt nicht kategorisierte Websites, die dann bewertet, einer Kategorie zugeteilt und in kürzester Zeit in die Websense-Datenbank aufgenommen werden.

Durch WebCatcher veranlasste Neueinträge werden allen Websense-Kunden im Rahmen der täglichen Datenbankupdates zugänglich gemacht. Somit profitieren alle Websense-Kunden von der Summe der

Surfgewohnheiten der Websense Kunden. Die Erfassung aller nicht kategorisierten URLs durch Kunden ist das bestmögliche Verfahren zur Gewährleistung einer vollständigen Abdeckung mit relevanten Internet-Filterfunktionen für das Employee Internet Management. Die WebCatcher-Funktionalität verbindet modernste Klassifizierungstechnologien mit einer Prüfung durch Mitarbeiter und stellt so ein Optimum an Präzision sicher. Das Ergebnis ist eine Kontrollliste, die sowohl einen maximalen Umfang als auch ein Höchstmaß an Genauigkeit bietet.

AppCatcher™, eine Funktion von CPM, gewährleistet, dass neue oder noch nicht klassifizierte Anwendungen und ausführbare Dateien, die von Mitarbeiter startet, einer Kategorie zugeordnet und in die Websense-Datenbank aufgenommen werden. AppCatcher bietet also für die Anwendungen des Kundenunternehmens dieselbe Funktionalität, die WebCatcher bei der Kategorisierung von URLs erbringt. AppCatcher stellt in der Praxis sicher, dass Websense bezüglich der Kategorisierung und Normierung ausführbarer Dateien und Anwendungen stets auf dem aktuellen Stand bleibt. Bei aktiviertem AppCatcher werden die Daten unbekannter ausführbarer Dateien automatisch und bei voller Gewährleistung des Datenschutzes an Websense übermittelt und von Fachleuten untersucht, einer Kategorie und einer Anwendung zugeordnet². Beim nächsten Download der CPM-Datenbank wird die Websense-Anwendungsliste aktualisiert. Daten bislang unbekannter Anwendungen und ausführbarer Dateien werden ergänzt, was deren automatische Kategorisierung und Anwendungszuordnung ermöglicht.

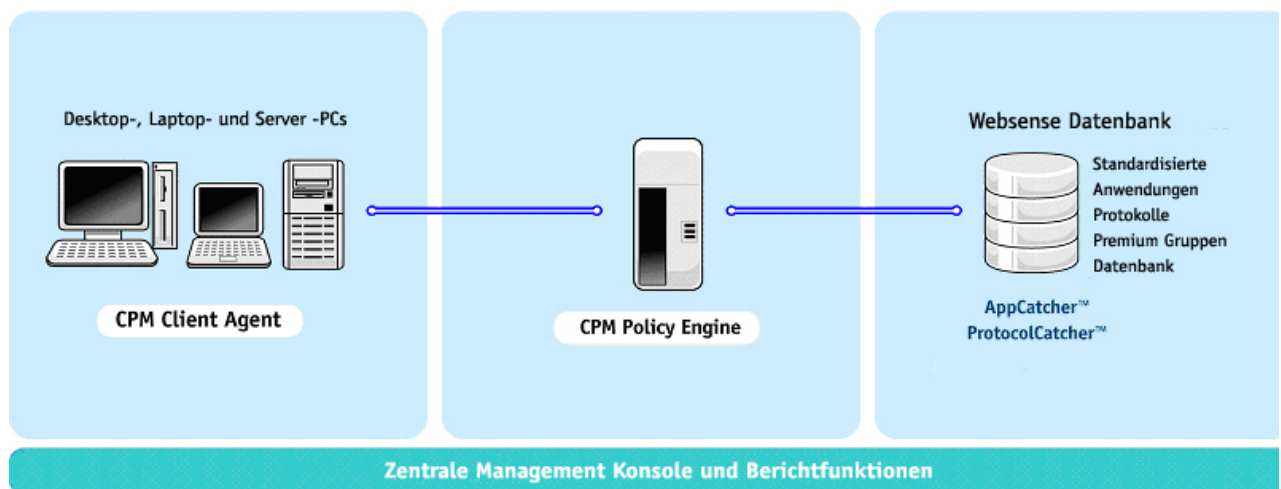


Abbildung 2: Der CPM AppCatcher sammelt, kategorisiert und ordnet unbekannte Anwendungen und ausführbare Dateien zu.

Sowohl WebCatcher als auch AppCatcher bauen auf den weltweit führenden Data-Mining-, Kategorisierungs- und Distributionstechnologien und der Erfahrung von Websense auf und gehören zum einzigartigen Leistungsumfang von Websense Enterprise.

² Bei der Anwendungskategorisierung werden unterschiedliche ausführbare Dateien unter dem Namen einer bestimmten Hauptanwendung aufgeführt. Microsoft Outlook besteht beispielsweise aus verschiedenen Anwendungskomponenten, die bei der Inventarisierung durch CPM alle unter der Anwendung „Microsoft Outlook“ geführt werden.

Fazit

Beinahe täglich werden neue Sicherheitslücken bekannt – ob im Zusammenhang mit den hier beschriebenen Web-Attacken, Spyware, Malicious Mobile Code oder Phishing-Angriffe. Die jüngsten Angriffe aus dem Internet weisen deutlich auf die Unzulänglichkeiten der Mehrzahl aller derzeit eingesetzten Sicherheitslösungen hin. Firewall-Lösungen am Gateway, die lediglich mit einer Antivirensoftware kombiniert sind, bieten keinen ausreichenden Schutz gegen die neuen komplexen, bösartigen Programme, die eine Bedrohung für IT-Infrastrukturen darstellen. Unternehmen können schlicht nicht vorhersehen, wie und wo der nächste Angriff erfolgt. Besonders wichtig ist in diesem Zusammenhang, dass vorausgeplant wird bzw. dass man geeignete Schutzmaßnahmen ergreift,

denn herkömmliche Sicherheitsvorkehrungen schützen nicht ausreichend vor neuen Gefahrenquellen. Unternehmen sollten ihre vorhandenen Sicherheitsvorkehrung um eine Lösung mit inhaltsbezogenen Managementfunktionen erweitern. Websense bietet einen solchen Schutz, der an drei unterschiedlichen Punkten wirkt: am Internet-Gateway, im Netzwerk und auf Desktopebene. Dieses mehrschichtige, inhaltsbezogene Konzept schützt Mitarbeiter und Computerumgebungen.

Besuchen Sie www.websense.de für weitere Informationen und eine Vollversion zum kostenlosen 30-Tage-Test.

Über Websense Inc.

Websense (NASDAQ: WBSN) ist der Weltmarktführer in Sachen Employee Internet Management. Mit Lösungen von Websense können Unternehmen die Nutzung von IT-Ressourcen optimieren und gleichzeitig die Risiken bei der Internetnutzung minimieren, zu denen auch Instant Messaging, Peer-to-Peer-Anwendungen und Spyware zählen. Durch eine Definition und Umsetzung von Nutzungsvorschriften am Internet-Gateway, im Netzwerk und auf Desktopebene steigern Produkte von Websense die Produktivität und Sicherheit, optimieren die Nutzung von IT-Ressourcen und minimieren Haftungsrisiken des Kunden. Weltweit schützt Websense mehr als 24.300 Kunden und 19,5 Millionen Mitarbeiter. Weitere Informationen erhalten Sie bei www.websense.de.

© 2004, Websense. Alle Rechte vorbehalten. Websense und Websense Enterprise sind Warenzeichen oder eingetragene Warenzeichen von Websense, Inc. Websense ist durch eine Reihe von Patenten weltweit geschützt. Alle sonstigen Warenzeichen sind Eigentum ihrer entsprechenden Firmen.