



Bedrohungsmanagement

Herausforderungen und Lösungen ↻

➔ Internet-Bedrohungen

Ein Trend Micro Whitepaper | Februar 2007

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

➔ INHALTSVERZEICHNIS

Kurzfassung	3
Einführung: Ein unwillkommenes Szenario	3
Hintergrund	4
Definition von Internet-Bedrohungen	4
Formen der Internet-Bedrohung	5
Hochentwickelte Methoden	5
Auswirkungen und Ausmaß von Internet-Bedrohungen	5
Traditionelle Ansätze bieten keinen Schutz vor Internet-Bedrohungen	8
Ein neuer Ansatz ist erforderlich: Integrierte, mehrschichtige Sicherheitslösung	8
In-the-Cloud (internetbasiert)	9
Am Internet Gateway	10
An den Endpunkten	11
Feed-Through und Loop-Back	11
Erweiterung dieses Ansatzes auf die E-Mail-Sicherheit	12
Fazit	13
Literaturhinweise	14

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

KURZFASSUNG

Angelockt von der Aussicht auf Gewinne aus dem Verkauf gestohlener vertraulicher Informationen gehen kriminelle Internet-Betrüger heutzutage dazu über, das weltweite Netz als Medium für ihre bösartigen Handlungen zu verwenden. Aufgrund ihrer komplexen Techniken, einem explosionsartigen Anstieg von Varianten und ihrer gezielten, regionalen Attacken können Internet-Bedrohungen auf vielfältige Weise potenzielle Kosten, einschließlich Identitätsdiebstahl, Verlust von vertraulichen Geschäftsinformationen, Schädigung der Markenreputation sowie einer Erosion des Kundenvertrauens in den Internet-Handel verursachen. Die Kombination dieser hohen Risiken mit der immer weiter verbreiteten Nutzung des Internets und der Komplexität eines Sicherheitsschutzes gegen Internet-Bedrohungen stellt die vielleicht größte Herausforderung für den Schutz der Privatheit persönlicher Informationen und der Vertraulichkeit von Geschäftsinformationen in den letzten zehn Jahren dar. Traditionelle Mittel bieten keine angemessene Sicherheit vor diesen Bedrohungen, und einzelne Methoden oder Techniken werden die Situation nicht verbessern. Stattdessen muss ein mehrschichtiges und umfassendes Bündel von Techniken angewendet werden. Dieses Whitepaper beschreibt Internet-Bedrohungen, wie sie funktionieren und welche Auswirkungen sie haben; erklärt, warum traditionelle Methoden angesichts dieser Bedrohungen versagen und beschreibt die erforderlichen Eigenschaften und Merkmale eines neuen Ansatzes.

EINFÜHRUNG: EIN UNWILLKOMMENES SZENARIO

Robert, ein Anwalt in der Rechtsabteilung eines großen pharmazeutischen Unternehmens, kommt Montag morgens in sein Büro, meldet sich an seinem Computer an und, wie es seine Gewohnheit ist, überfliegt als erstes seine neuen E-Mails. Der Basketballfan Robert hatte sich am Abend zuvor im Fernsehen ein Spiel angesehen. Während er noch über das Spiel nachdenkt, bemerkt er die kurze E-Mail eines Freundes. Die Nachricht beinhaltet einen Link zu einer neuen Internetseite mit Informationen über einen seiner Lieblings-Basketballspieler. Robert folgt also dem Link, der ihn zu einer faszinierenden Website mit Fotos, Videos und weiteren Informationen über den Spieler führt. Doch während sein Browser eines der Fotos aufbaut, führt ein bösartiger Code, der in der jpg-Datei enthalten ist, durch den Anwalt unbemerkt den Befehl aus, eine ausführbare Datei herunterzuladen, die auf seinem Computer automatisch startet. Diese Malware greift dann auf vordefinierte Dateitypen zu, die auf Roberts Festplatte gespeichert sind, komprimiert und verschlüsselt sie und sendet sie an die E-Mail-Adresse eines Dritten – die Adresse des Internet-Betrügers. Einige dieser Dateien beinhalten hochvertrauliche Informationen über verschiedene Patentverfahren, in denen Robert beteiligt ist. Indem er die gleiche E-Mail an eine Liste von Mitarbeitern in verschiedenen pharmazeutischen Unternehmen schickt, zielt der Internet-Betrüger speziell auf die Pharmaindustrie, um an solche Informationen heranzukommen und sie anschließend Gewinn bringend zu verkaufen. Durch einen einzigen Klick auf die scheinbar harmlose Verknüpfung zu der Website hat Robert also unbeabsichtigt einen Prozess in Bewegung gesetzt, durch den vertrauliche Geschäftsinformationen in falsche Hände geraten. Dies kann für sein Unternehmen den Verlust wettbewerbsfähiger Patente, rechtliche Verstrickungen und weitere Kosten bedeuten.

Am selben Montagmorgen überwacht eine IT-Administratorin des pharmazeutischen Unternehmens den Netzwerkverkehr. Darauf vertrauend, dass das Unternehmen kürzlich seine Client-basierte Antiviren-Software durch eine URL-Filter-Liste ergänzt hat, kann die Administratorin keinerlei ungewöhnliche Aktivitäten auf ihrem Bildschirm feststellen. Der Download der Malware und der daraus folgende Diebstahl von Roberts Dateien bleibt aus mehreren Gründen, die mit den heute üblichen Vorgehensweisen von Internet-Dieben zusammenhängen, unentdeckt. Zunächst hat der Schreiber der Malware die neue Internetseite mit dem bösartigen Inhalt erst an diesem Morgen ins Netz gestellt, so dass sie in der Liste des URL-Filters nicht aufgeführt ist. Außerdem hat der Internet-Betrüger in die Malware den Befehl eingebaut, Roberts Dateien nach und nach zu exportieren, wodurch ein ungewöhnlicher Anstieg des Netzwerkverkehrs, der vom Administrator bemerkt werden könnte, vermieden wird. Da das pharmazeutische Unternehmen am Gateway keine Software mit Verhaltensanalyse installiert hat, werden die E-Mails mit Anhängen, die aus dem Computer des Anwalts sickern, nicht als außergewöhnlich erkannt.

Unglücklicherweise spielen sich derartige Szenarios auf der ganzen Welt sowohl in großen Konzernen wie auch in kleinen Firmen ab. Eine große und ständig wachsende Zahl so genannter „Internet-Bedrohungen“ wie die oben beschriebene, aber in unendlichen Variationen, richtet verheerende Schäden an. Internet-Betrüger stehlen Listen mit Sozialversicherungsnummern in Gesundheitsorganisationen, Kreditkartennummern in Finanzinstituten und firmeneigene Informationen in Unternehmen der Technischen Industrie. Diese Diebstähle ermöglichen nicht nur den Identitätsdiebstahl: sie untergraben das Vertrauen der Kunden in den Datenschutz, in das Online-Banking, in Transaktionen über Internet und E-Commerce.

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

HINTERGRUND

Im Verlauf der letzten 15 Jahre haben sich die Bedrohungen für die Datensicherheit in immer neuen Formen weiterentwickelt. Viren, die in heruntergeladenen ausführbaren Dateien eingebettet waren, machten Makroviren in Dokumentdateien Platz, einige Jahre später folgten Bedrohungen, die per E-Mail versendet werden (z. B. die Viren „I Love You“ und „Melissa“). In allen Fällen machten die Schreiber von Malware dasjenige Medium ausfindig, das am meisten genutzt und am wenigsten geschützt war. Nach wie vor kann Malware den zunehmenden Gebrauch von E-Mails ausnutzen, doch die wachsende Erkenntnis, dass ein solcher Schutz notwendig ist, führte zu verstärkter und sich weiter verbessernder Sicherheit dieser Übertragungsmöglichkeit. Heute taucht eine neue Welle von Bedrohungen auf, die das Netz als Transportmedium verwenden.

Entsprechend den Entwicklungen in der Vergangenheit gewinnen Internet-Bedrohungen zu einem Zeitpunkt an Boden, an dem der Gebrauch ihres Mediums – des Internets – am weitesten verbreitet, zu einem wachsenden Motor des Handels geworden und im Wachstum begriffen ist. Die meisten Büroarbeiter starten als allererstes ihren Browser auf dem Desktop; so beginnen die meisten Menschen ihre Arbeit. Gesellschaftliche Trends wie Myspace und YouTube sowie ein zunehmend regionales Verhalten der Internetnutzer sind wichtige Aspekte dieser Internetnutzung.

Gleichzeitig ist das Netz als Medium zur Verbreitung von Malware relativ ungeschützt, im Vergleich zum Bereich der Nachrichtenübermittlung. Laut IDC sind „bis zu 30% der Unternehmen mit 500 oder mehr Mitarbeitern als Folge des Surfens im Internet infiziert worden, während nur 20%-25% derselben Unternehmen Viren oder Würmer durch E-Mails erhielten.“ [1] Aufgrund der viel größeren Bandbreite, die zum Durchsuchen oder Filtern seines Datenstroms erforderlich ist, ist Sicherheit im Internet weitaus schwieriger zu gewährleisten als in E-Mails, die weniger als ein Tausendstel der Datenmenge beinhalten. Obwohl nach wie vor wichtig für die Sicherheit beispielsweise der Client-Computer vor zahlreichen Bedrohungen, bieten traditionelle Antiviren-Programme, die auf diesen Clients installiert sind, keinen ausreichenden Schutz gegen die sich weiter entwickelnden Internet-Bedrohungen. Dies führt zu „idealen Bedingungen“ für das Vorrücken von Internetbedrohungen: ein relativ ungeschütztes, aber weit verbreitetes und ständig genutztes Medium, das entscheidend für die Produktivität eines Unternehmens ist. Folglich befindet sich die Daten- und Informationssicherheit heute an einem kritischen Wendepunkt: ein neuer Ansatz ist erforderlich, um der neuesten Form der Bedrohungen entgegenzutreten.

DEFINITION VON INTERNET-BEDROHUNGEN

Internet-Bedrohungen umfassen eine große Zahl von Bedrohungen aus dem Internet. Sie zeichnen sich durch ausgeklügelte Methoden aus und nutzen eine Kombination verschiedener Dateien und Techniken anstatt nur einen einzelnen Ansatz oder Dateityp. Die Urheber von Internet-Bedrohungen ändern beispielsweise ständig die verwendete Version oder Variante. Da eine Internet-Bedrohung eher am festen Ort einer Internetseite gespeichert ist und nicht auf dem infizierten Rechner des Nutzers, muss ihr Code ständig verändert werden, um nicht entdeckt zu werden.

In den letzten Jahren werden Personen, die einst „Hacker“ genannt wurden, Virenschreiber, Spammer sowie Hersteller von Spyware lediglich als Internet-Betrüger bezeichnet. Diese Kriminellen setzen Internet-Bedrohungen vor allem ein, um finanziellen Gewinn zu erzielen. Dies erreichen sie, indem sie eine Infektion der Geräte durch einfache Nutzerbesuche auf gezielten Websites verursachen und sich anschließend mit Hilfe verschiedener Tarntechniken in einem Computer oder im Netz verstecken. Einmal platziert, stiehlt der bösartige Code langsam und heimlich die Dateien des Nutzers und verbraucht Computerleistung.

„Ideale Bedingungen“ für das Vorrücken von Internet-Bedrohungen: ein relativ ungeschütztes, aber weit verbreitetes und ständig genutztes Medium, das entscheidend für die Produktivität eines Unternehmens ist.

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

➔ Formen der Internet-Bedrohung.

Nachfolgend sind einige Beispiele dieser Gruppe von Bedrohungen aufgeführt, die nach verschiedenen Teilen des Lebenszyklus einer Bedrohung kategorisiert sind.

- Wie die Internetverknüpfungen geliefert werden
 - Spam, Phishing-Angriffe per E-Mail, „werden Sie schnell reich“-Betrugsversuche und alle anderen zielgerichteten E-Mails, die URLs beinhalten und den Nutzer zu einer bösartigen Internetseite führen
 - Ein manipulierter Domain Name Server (DNS-Poisoning, z.B., mittels Pharming) oder manipulierte Internetseiten, die den Benutzer auf betrügerische Websites (anstatt zu den richtigen) oder Proxy-Server leiten, um entweder Informationen zu stehlen oder den Benutzer zu infizieren
 - Social Networking Sites und verschiedene andere Möglichkeiten, den Benutzer zu überlisten und infizieren
- Schädigung über die Website
 - Schwachstellen in Mediendateien (z.B. Bilder, Animationen, Videos und Audiodateien) bei der Wiedergabe durch den Browser, durch die bösartige Dateien eingeschleust oder heruntergeladen werden
 - ActiveX-Steuerelemente oder unbemerkte Downloads, die den Benutzer entweder dazu zwingen Dateien herunterzuladen, um sie weiter ansehen zu können, oder die automatisch eine bösartige Datei übertragen, wenn ein ungeschützter Browser verwendet wird
- Infektionsroutine
 - Infektion durch Anwendungen, die bösartige Dateien in ein System einschleusen
 - Häufige selbstständige Aktualisierung der Internet-Bedrohung durch Download von mehreren Code-Sätzen, um mit traditioneller Antiviren-Software nicht entdeckt werden zu können
- Schadensfunktionen nach der Infektion
 - Spyware oder Anwendungen, die Informationen oder Daten aus einem System stehlen und sie an Dritte versenden
 - Adware, Data Miner, oder Pop-ups zu Werbezwecken
 - Browser-Hilfsobjekte, die die Resultate von Suchmaschinen manipulieren oder die Surfgewohnheiten des Benutzers überwachen, um Informationen über die Interessen des Benutzers zu sammeln (z. B. Waren oder Dienstleistungen) und Werbeanzeigen zu platzieren
 - Bots (Code, der ferngesteuert bösartige Aktionen ausführen kann) oder Zombies, die über das Internet Befehle empfangen können

➔ Hochentwickelte Methoden.

Internet-Bedrohungen nutzen typischerweise Internet-Port 80 aus, der fast ständig offen ist, um Zugang zu den Informationen, Kommunikationsmöglichkeiten und der Produktivität zu ermöglichen, die das Internet den Mitarbeitern bietet. (Das vorherige Beispiel illustriert diesen Ansatz.) Varianten der Internet-Bedrohungen verfolgen die Taktik einer Infektion auf regionaler oder lokaler Ebene (z.B. über lokale Sprachenseiten, die sich an bestimmte Bevölkerungsgruppen richten) und verwenden nicht die Technik der Masseninfizierung früherer Malware-Vorgehensweisen. Malware-Autoren greifen auch zu Methoden des Social Engineering und überlisten Benutzer mit verlockenden Betreffzeilen in E-Mails (die oft die URL einer Website beinhalten, die bösartige Codes herunterlädt) zu Urlaub, Prominenten, Sport, Pornografie, Weltgeschehen und anderen beliebten Themen.

AUSWIRKUNGEN UND AUSMASS VON INTERNET-BEDROHUNGEN

Internet-Bedrohungen dienen Kriminellen zur Verfolgung eines von zwei Zielen. Ein Ziel ist der Diebstahl von Informationen und ihr Verkauf. Auswirkungen sind in erster Linie der Verlust vertraulicher Informationen in Form von Identitätsverlust oder die Benutzung des infizierten Users als Überträger für Phishing-Mails oder andere Information beschaffende Aktivitäten. Diese Bedrohung kann unter anderem dazu führen, dass das Vertrauen in den Internethandel und für Internet-Transaktionen schwindet und beschädigt wird. Das zweite Ziel besteht darin, die Leistung des Benutzercomputers zu „rauben“, um es als Instrument für gewinnträchtige Aktivitäten zu missbrauchen, wie zum Beispiel das Versenden von Spam oder Erpressung in Form von verteilten Denial-of-Service-Angriffen oder Pay-per-click-Aktivitäten.

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

Die Gewinne, die mit Hilfe verschiedener Internet-Bedrohungen erzielt werden, sind erheblich. Jeanson James Ancheta zum Beispiel verdiente \$60,000 USD mit einem 400.000-PC Botnet [2]. Ivan Maksakov, Alexander Petrov und Denis Stepanov erpressten 4 Millionen US-Dollar mit Hilfe eines verteilten Denial-of-Service-Angriffs auf Sportwetten-Buchmacher in Großbritannien [3]. Auf dem Schwarzmarkt für solche Malware werden Preise von 1000-5000 US-Dollar für ein Trojanisches Pferd gezahlt, das beispielsweise zum Diebstahl von Online-Kontoinformationen in der Lage ist [4]. Über das wahre Ausmaß der Gewinne in diesem Untergrundsektor ist wegen seines geheimen Charakters natürlich nicht viel bekannt.

Dennoch konnten einige aggregierte Daten zu den finanziellen Auswirkungen einiger webbasierter Bedrohungen gesammelt werden. Der Verbraucherbericht aus den USA führt auf, dass Phishing-Angriffe auf US-Bürger im Jahre 2005 einen Schaden von 630 Millionen US-Dollar verursachten [5]. Trotz des Gebrauchs von Transaktionsnummern (TANs) in Verbindung mit Benutzernamen und Passwörtern wurden Kunden von diversen deutschen Banken Opfer von Phishing-Attacken. Die Münchener Polizei schätzt den Schaden durch Internetbetrug (Januar bis Juli 2006) auf über 1 Million Euro allein in München [6]. Laut Asia.Internet berichtet die Gartner Group, dass sich der Gesamtschaden durch Phishing im Jahre 2006 auf 2,8 Milliarden Dollar beläuft [7].

Die Abbildungen 1 und 2 zeigen Schätzungen des Umfangs verschiedener Internetbedrohungen. Gleichzeitig deuten die Daten darauf hin, dass sich die Zahl der Internet-Bedrohungen erhöht (siehe Abb. 3). Die Standard Bank schätzt, dass die Menge an Spyware in den letzten 18 Monaten um 50 Prozent gestiegen ist und sich die Virenproduktion in den letzten drei Jahren versechzehnfacht hat [8]. Eine Studie zeigte, dass Phisher innerhalb von nur 24 Stunden mit bis zu 14 Prozent ihrer Betrugsnachrichten erfolgreich sein können – das ist eine viel höhere Quote als von Beobachtern der Netzwerksicherheit früher geschätzt [9].

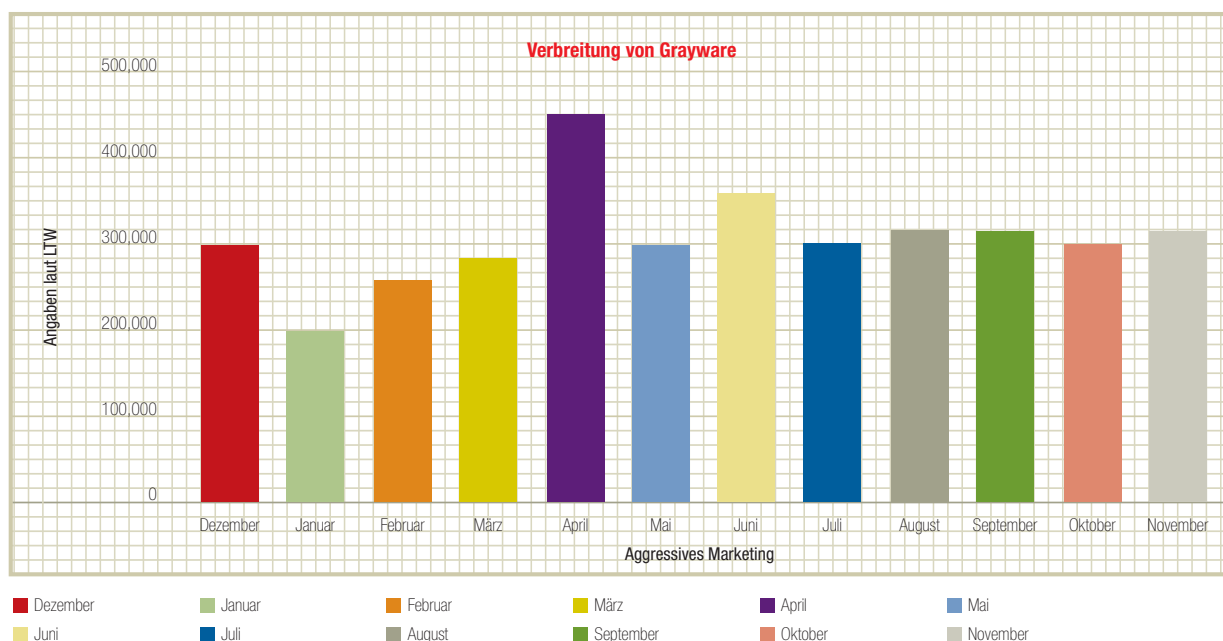


Abbildung 1. Die Verbreitung von Grayware – die als ungefährlich eingestuft wurde – stieg im Jahre 2006 signifikant an. Dies ist ein Grund zur Besorgnis, da Trend Micro die Tendenz zum Einsatz von Malware als Mittel zur Erzielung von Gewinnen per Click-through festgestellt hat. *Quelle: Trend Micro*

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

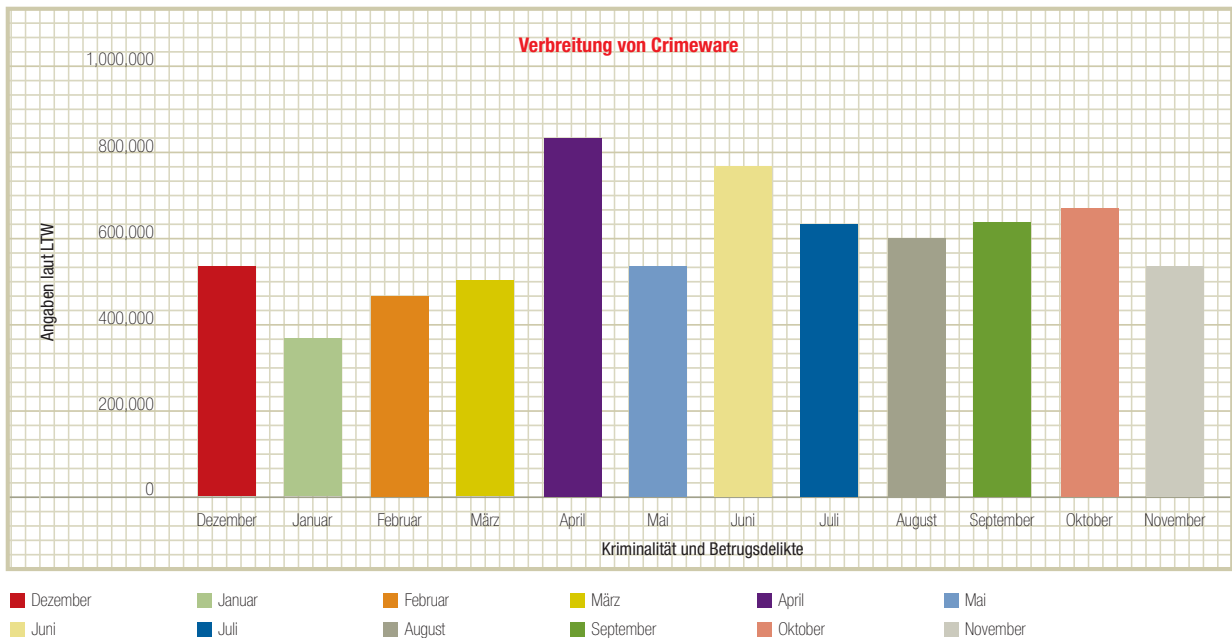


Abbildung 2. Im Jahr 2006 stieg die Verbreitung von Crimeware – für Wirtschaftskriminalität entwickelte, bösartige Software – signifikant an. *Quelle: Trend Micro*

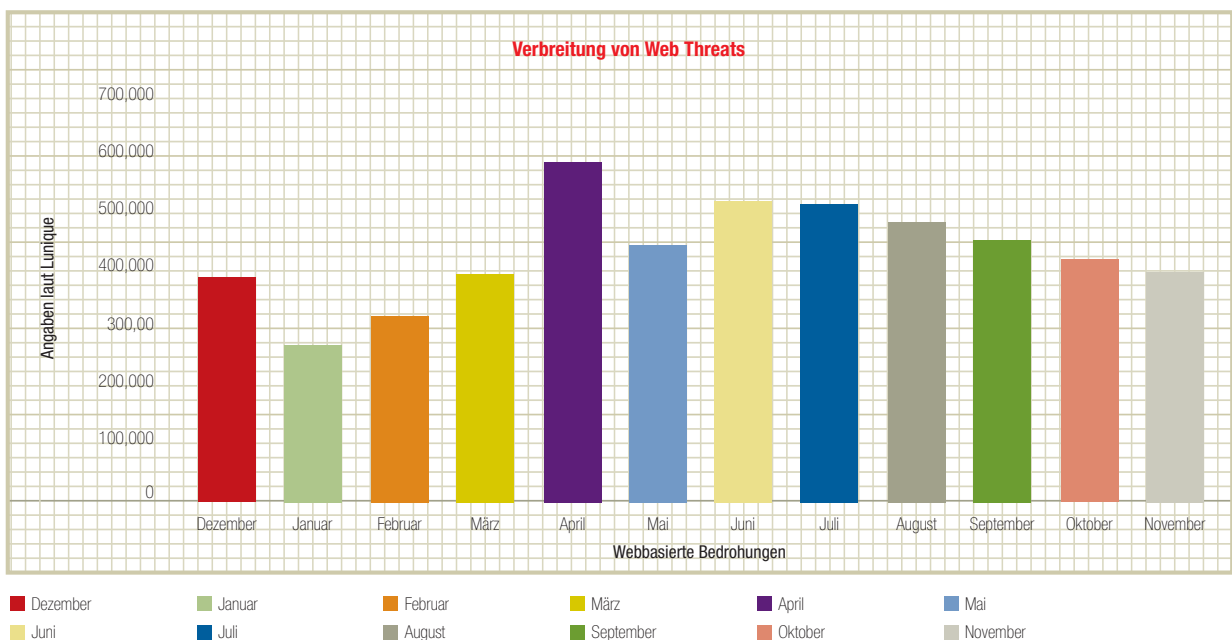


Abbildung 3. Nach E-Mail ist das Internet das am meisten verbreitete Mittel zur Verbreitung von Malware. *Quelle: Trend Micro*

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

TRADITIONELLE ANSÄTZE BIETEN KEINEN SCHUTZ VOR INTERNET-BEDROHUNGEN

Die traditionelle Methode des Virenschutzes besteht darin, dass Virenproben gesammelt und Muster entwickelt werden, die anschließend schnell an die Benutzer verteilt werden. Dies ist für die Abwehr von Internet-Bedrohungen aus mehreren Gründen nicht ausreichend.

Zum Beispiel, weil viele Internet-Bedrohungen zielgerichtete Angriffe sind und zahlreiche Varianten umfassen, wodurch es nahezu unmöglich wird Proben zu sammeln. Die zahlreichen Varianten verwenden mehrere Transportvehikel (z. B. Spam, Instant Messaging und Websites) wodurch sie den traditionellen Prozess des Sammelns von Proben und Entwickelns von Mustern unschädlich machen. Da Internet-Bedrohungen eine Vielzahl an Taktiken verwenden (z.B. zielgerichtete lokale und regionale Angriffe, Spam in lokalen/regionalen Sprachen, Websites), kann eine Sicherheitslösung allein nicht auf alle Bedrohungen passen; ein gesammeltes Muster für einen gezielten lokalen Angriff kann anderen lokalen Attacken nicht entgegenreten.

Grundsätzlich versuchen Internet-Bedrohungen sich zu verstecken, anstatt zu erkunden und sich auszubreiten, und sind daher mit traditionellen Antiviren-Techniken schwierig zu entdecken. In einigen Fällen können Internet-Bedrohungen ein solches Ausmaß annehmen (z.B. über ein Rootkit, in dem die Systemdatei ersetzt wird), dass herkömmliche Deinstallations- oder Systemsäuberungsansätze nutzlos werden. Oft ist dann eine komplette Wiederherstellung erforderlich: die Festplatte muss gelöscht, das Betriebssystem, die Anwendungen und Benutzerdaten neu installiert werden. Internet-Betrüger nutzen außerdem aus, dass Port 80 für den regulären Verkehr offen sein muss, wodurch vorhandene Client Firewalls umgangen werden. Und einige professionelle Internet-Betrüger verwenden die Verwundbarkeit des „Pre-Zero Day“, so dass nicht einmal On-time Sicherheitspatches die Wirkung dieser Bedrohungen verhindern können.

Gleichzeitig nehmen profitgierige Internet-Betrüger nicht nur die Windows Webserver-Plattform (um z.B. eine Download-Quelle zu verteilen) ins Visier, sondern gefährden auch andere Plattformen. Tatsächlich arbeiten Web Threats systemunabhängig und greifen jede Art Webserver an. Dies bedeutet, dass sogar Linux-basierte Webserver gefährdet sind, von denen früher angenommen wurde, dass sie für Sicherheitsbedrohungen weniger anfällig sind. Einmal installiert, startet das Malware-Programm weitere Programme, um die Regeln des Host Intrusion Prevention Systems (HIPS) zu verletzen. Exzessive Fehlerwarnungen verärgern den Benutzer so sehr, dass dieser den Schutz deaktiviert oder die Ausführung des Programms erlaubt. Auf diese Weise umgeht die Malware traditionelle HIPS-Techniken.

Einzelne Download-Programme – für gewöhnlich als Teile von Web Threats verwendet – scheinen harmlos zu sein. In Kombination werden sie allerdings bösartig und führen dazu, dass die dateibasierte heuristische Suche nutzlos wird oder Fehlalarme verursacht werden. Internet-Bedrohungen erweitern diese Technik oft und ergänzen sie durch mehrschichtige, Multi-Protokoll koordinierte Angriffe, um die Entdeckung durch herkömmliche Methoden zu vermeiden. Ein Internetbetrüger integriert zum Beispiel eine URL in eine Webmail oder Instant Message. Der Benutzer klickt auf den Link zu einer rechtmäßigen URL, die der Internet-Betrüger für die Dauer von einigen Tagen oder Stunden „entführt“ (hijacked) hat. Anschließend testet ein ActiveX-Steuerelement die Verwundbarkeit des Browsers des Benutzers. Wird eine Schwachstelle entdeckt, greift die Malware an; falls nicht, lädt eine Datei herunter, sucht nach Schwachstellen, lädt weitere Dateien herunter, und so fort. Die einzelnen Teile des Verkehrs scheinen ungefährlich zu sein, die kombinierten Aktivitäten aber werden zu einer koordinierten Attacke.

EIN NEUER ANSATZ IST ERFORDERLICH: INTEGRIERTE, MEHRSCHICHTIGE SICHERHEITSLÖSUNG

Es ist klar: Zum Schutz vor Internet-Bedrohungen ist ein neuer Ansatz erforderlich, der die bereits existierenden Techniken ergänzt. Die effektivste Methode setzt ein mehrschichtiges Sicherheitssystem ein und beinhaltet eine ganze Reihe von Sicherheitsmaßnahmen. Zusätzlich erfordert die Wandlungsfähigkeit der Threats eine Art Feedback-Funktion, durch die Informationen, die in einem Teil des Sicherheitssystems gesammelt wurden, zur Aktualisierung in anderen Schichten eingesetzt werden können. Ein effektiver Sicherheitsansatz sollte sich aufgrund der Fähigkeit der Internet-Bedrohungen Protokolle einzusetzen außerdem mit all den relevanten Protokollen befassen. Um diese Maßnahmen zu koordinieren, ist ein effizientes, zentralisiertes Management erforderlich, und selbstverständlich könnte man dem regionalen und sogar lokalen Charakter vieler Bedrohungen begegnen, wenn bestimmte Regionen der Welt mit regionalem Know-How gezielt angegangen würden.

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN



Abbildung 5. „In the cloud“ besteht die Aufgabe darin, die Vertrauenswürdigkeit jeder Website in mehreren umfangreichen Arbeitsschritten zu prüfen.

➔ Am Internet-Gateway.

Auch auf der zweiten von drei Ebenen, dem Internet-Gateway, sind wichtige Funktionen erforderlich. Die Gateway-Funktionen sollten eine Dateiprüfung beinhalten, die entweder mit Hilfe einer Software- oder Hardware-Appliance durchgeführt werden kann. Die Dateiprüfungsfunktion prüft im Wesentlichen die Vertrauenswürdigkeit jeder Datei, bevor dem Benutzer ihr Download erlaubt wird. Zu diesem Zweck werden die Daten aller Dateien auf der Internetseite abgetastet, und es wird regelmäßig eine Bewertung der Vertrauenswürdigkeit jeder Datei durchgeführt, um eine Datenbank zur Vertrauenswürdigkeit von Dateien zu erstellen und zu pflegen. Diese Überprüfung der Dateien neben der Prüfung der Vertrauenswürdigkeit einer Website in-the-cloud ist deshalb so wichtig, weil Internet-Betrüger Dateien mit böartigem Inhalt problemlos von einer Internetseite zur nächsten verschieben können.

Die zweite Funktion zum Schutz vor Internet-Bedrohungen, die am Gateway benötigt wird, ist eine Art „Verhaltensanalyse“, die verschiedene Aktivitäten miteinander kombinieren kann, um herauszufinden, ob sie in der Gesamtheit böartig sind. Diese Analyse kann eine Art „Bewertungsnote“ für jede Kombination von Aktivitäten erstellen und eine Kombination blocken, sobald ihre Bewertung einen bestimmten Grenzwert überschreitet. Dieser Ansatz kann auch Auslöser identifizieren, die als Anhaltspunkte oder Hinweise in Sitzungsdaten oder einer Protokolleigenschaft auftreten und dazu verwendet werden können, um verdächtige Aktivitäten zu entdecken. Darüber hinaus kann dieser Ansatz Regeln am Gateway für eine Korrelation von Auslösern, die zu definierten Bedingungen böartiger Aktivitäten passen, implementieren.

Dieser Ansatz muss beispielsweise Aktivitäten einer einzelnen Sitzung im selben Protokoll (z.B. ein SMTP-Anhang mit verdächtiger doppelter Erweiterung) miteinander in Beziehung setzen. Der Ansatz sollte auch Aktivitäten während Sitzungen mit mehreren Netzwerkverbindungen im selben Protokoll miteinander korrelieren (z.B. eine komplexe Download-Bedrohung, in der einzelne Dateien harmlos erscheinen, aber in Kombination ein böartiges Programm darstellen). Sogar Aktivitäten in mehreren Sitzungen und verschiedenen Protokollen (z.B. SMTP und HTTP) sollten korreliert werden, um verdächtige Aktivitätenkombinationen (z.B. eine E-Mail mit einer URL-Verknüpfung zu mehreren Empfängern und dem Download einer ausführbaren Datei von dieser Verknüpfung in HTTP).

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

➔ An den Endpunkten.

Trotz der Implementierung dieser Maßnahmen in-the-cloud und am Gateway bleibt die dritte Ebene der Endgeräte (z.B. Client) ein Sicherheitsrisiko. Etwa zwei Drittel der aktuellen Verkäufe von Computerhändlern sind Notebooks [10]. Diese Geräte benötigen Sicherheitsschutz, weil sie sich an verschiedene Netzwerke anschließen und Besucher und Zulieferer sie physisch außerhalb des Gateways des Unternehmens verwenden; die Web Security Richtlinien des Unternehmens müssen unabhängig davon, ob der Benutzer sich in oder außerhalb des Netzwerkes befindet, durchgesetzt werden. Deshalb wird eine Lösung benötigt, die Sicherheitsschutz auf der Client-Ebene (z.B. Zugriffskontrolle und Suche) sowie Säuberungs- und Wiederherstellungsfunktionen für den Fall einer Infektion bietet. Wenn beispielsweise ein Notebook irgendwo manipuliert wurde und Teil eines Bot-Netztes ist, könnte das Notebook versuchen sich wieder mit dem Bot-Herder (dem Urheber des Bot-Netztes) zu verbinden. Ein weiteres Beispiel ist Spyware zum Versenden ausspionierter Daten (phone-home), die in regelmäßigen Abständen versucht, die im infizierten Computer gesammelten Informationen an den Besitzer der Spyware zu übertragen. In beiden Fällen können solche Aktivitäten entdeckt werden. Anschließend wird, falls erforderlich, eine Säuberung vorgenommen.

Sicherheitsschutz für Endgeräte sollte URL-Filter, Prüfung der Vertrauenswürdigkeit von Websites und den Einsatz eines „Wiederherstellungspunkts“ für das Gerät, der vor Beginn des Internetzugriffs gespeichert wird, umfassen. Durch die Verwendung des Wiederherstellungspunktes kann ein Benutzer, der nach dem Download einer Datei oder nach dem Surfen im Internet ungewöhnliche Aktivitäten feststellt, den Computer wieder auf diesen vorher gespeicherten Zustand zurückversetzen. Weitere vorbeugende Optionen sollten die Erstellung einer „virtuellen Umgebung“ beinhalten, mit der der Benutzer im Internet surft; diese Maßnahme führt dazu, dass Internet-Bedrohungen nur die virtuelle Umgebung erreichen und nicht in die tatsächliche Umgebung des Benutzers eindringen.

Säuberungsfunktionen sollten zwei Arten umfassen: Agentenbasierte und agentenlose Säuberungsmethoden. Bei Verwendung einer agentenbasierten Lösung sitzt ein zentral verwalteter Agent im Notebook, der die Aktivitäten koordiniert. Die agentenlose Methode gilt in Situationen, in denen kein Agent auf dem tragbaren Computer eines Besuchers oder Zulieferers installiert ist; in diesem Fall wird die Säuberung on-demand mit Hilfe von Zugriffskontrollen auf das Netzwerk (die z.B. nur beschränkten Zugriff auf das Netzwerk erlauben, um die Säuberung auszuführen) ausgeführt. Eine komplette Wiederherstellung ist ebenso erforderlich für Fälle, in denen zum Beispiel aufgrund einer Rootkit-Infektion keine Säuberung mehr durchführbar ist.

➔ Feed-Through and Loop-Back.

Abbildung 6 illustriert diesen mehrschichtigen Ansatz und zeigt außerdem einen wichtigen Aspekt für seine Implementierung. Die Vereinigung von Schutzschichten in-the-cloud, am Gateway und an den Endgeräten ist eine „Feed-through“-Vorrichtung. Die Rückmeldung von Informationen von einer Schicht zur anderen ist außerdem eine „Loop-back“-Vorrichtung. Informationen beispielsweise, die bei der Analysefunktion am Gateway ermittelt wurden, können rückgemeldet werden, um die Datenbanken zur Vertrauenswürdigkeit von Internetseiten oder die Funktionen an den Endgeräten zu aktualisieren. Ähnlich kann Information, die an den Endgeräten erlangt wurde, zu den Dateisuchfunktionen am Gateway oder an die Schutz- und Prüffunktionen „in-the-cloud“ zurückgemeldet werden. Sowohl die Technik des „Feed-through“ wie auch die des „Loop-back“ sind für kontinuierliche und angemessene Sicherheit erforderlich.

All diese Leistungsfunktionen und relevanten Richtlinien müssen von einer Konsole zur zentralen Steuerung überwacht und verwaltet werden. Gleichzeitig müssen sich bestimmte Teams auf bestimmte Regionen auf der Welt spezialisieren. Diese Teams sollten bei der Beschaffung von Informationen und Proben, bei der Schadensbegrenzung und Vorbeugung, und bei der Zusammenarbeit mit lokalen Sicherheitsgruppen und Vollstreckungsbehörden im Kampf gegen Internet-Bedrohungen an vorderster Reihe arbeiten. Ergebnis dieses Ansatzes werden schnellere Reaktionszeiten, kundenspezifische Lösungsmöglichkeiten und die Berücksichtigung kultureller Merkmale sein.

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

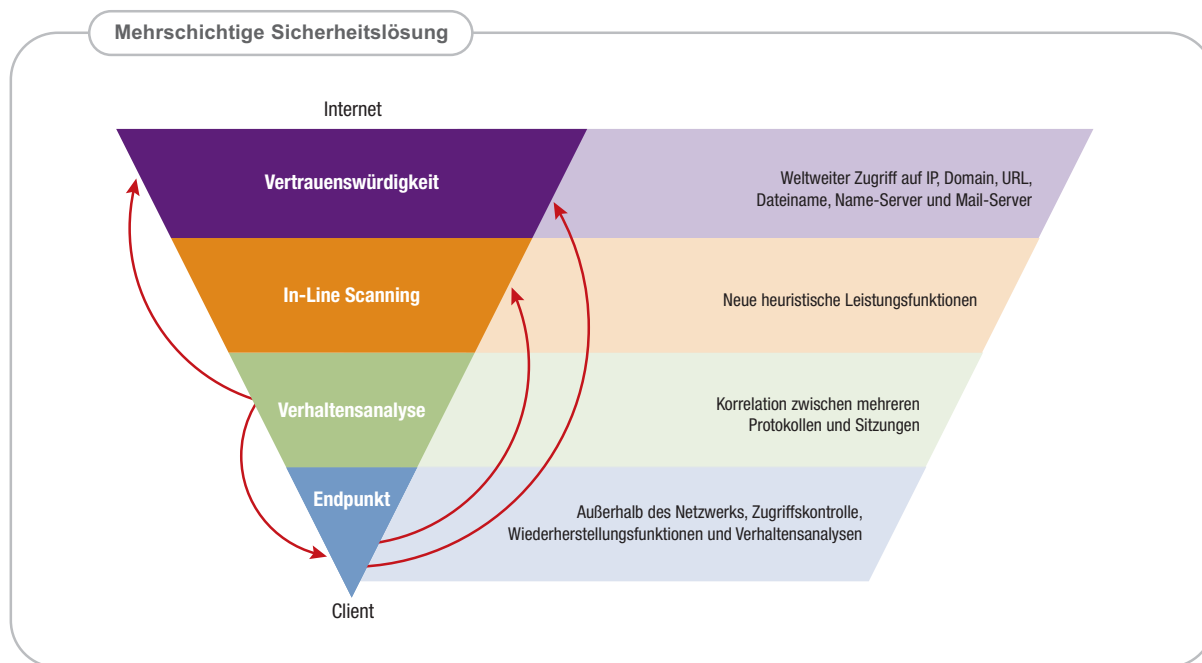


Abbildung 6. „Feed-through“ (von oben nach unten) und „Feedback“ (Pfeile) sind die Prinzipien, die einen mehrschichtigen Ansatz von „in-the-cloud“ über das Gateway, das Netzwerk, bis hin zu den Endpunkten, ergänzen.

ERWEITERUNG DIESES ANSATZES AUF DIE E-MAIL-SICHERHEIT

Dieser mehrschichtige Ansatz kann auch auf die E-Mail-Sicherheit ausgedehnt werden. Ein aktiver Schutz „in-the-cloud“ im Bereich Messaging ist wichtig, weil behördliche Auflagen die Zurückhaltung von E-Mails für den Zeitraum von zehn Jahren vorschreiben, sobald die E-Mail das Internet-Gateway erreicht. Eine Vorfilterung von E-Mails „in-the-cloud“ spart folglich Bandbreite, reduziert Speicher- und Wartungskosten und dient der Sicherheit. Auf dieser Ebene sollte der Sicherheitsschutz Prüfungsfunktionen für die Vertrauenswürdigkeit der E-Mail Sender-IPs und Domain-IPs, eine E-Mail-Firewall, sowie Anti-Spam- und Antiviren-Filter (mit hoher Trefferquote in dieser Schicht) umfassen. Die E-Mail-Firewall sollte nicht auf dem E-Mail-Server gehostet werden, um verteilte Denial-of-Services-Angriffe und unzulässige Zugriffe auf Verzeichnisdienste (z.B. Angriffe, die zufällig nach gültigen E-Mail-Adressen suchen) abzuwehren.

Am Internet-Gateway sollte die Anti-Spam und Antiviren-Software eine Virensuche für Dateianhänge beinhalten – ein relativ neuer Typ Bot-generierter Spam-Mails, der sehr schwer zu identifizieren ist, verwendet Bilder, um Spam zu tarnen, verbraucht Speicherkapazität und beinhaltet im Allgemeinen Malware. Auf dieser Ebene ist außerdem ein Policy-Engine erforderlich, die von den E-Mail-Servern aus mit dem Verzeichnis (z.B. LDAP) verknüpft ist. Hier kann durch Verhaltensanalyse entdeckt werden, dass ein Benutzer beispielsweise auf wiederholte E-Mails niemals antwortet, wodurch sie als Spam gekennzeichnet und zurückgeschickt werden können. E-Mail-Content-Suche kann auf dieser Ebene ebenfalls durchgeführt werden, um sicherzustellen, dass Mitarbeiter oder andere Unbefugte keine vertraulichen Informationen in E-Mails oder Dateianhängen enthüllen. Dieser Funktionsbereich sollte außerdem Verschlüsselung von ausgehenden E-Mails ermöglichen und E-Mail-Archivierung in Übereinstimmung mit den behördlichen Auflagen.

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

In der Messaging-Umgebung ist die dritte Ebene (die der Endpunkte) der E-Mail-Server selbst, da die Postfächer sich auf diesem Server befinden. Der E-Mail-Server muss Sicherheits-Software ausführen und den Endbenutzern die Möglichkeit geben Funktionen, wie zum Beispiel Quarantänepostfächer für Endbenutzer, zu verwalten, in die Spam-Mails gesendet werden. Diese zusätzliche Schutzschicht ist wichtig zur Abwehr von internen Messaging-Bedrohungen.

Da E-Mail und Internet-Bedrohung verschmelzen, werden Lösungen benötigt, die einen Austausch zwischen diesen Übertragungswegen bieten und Netzwerke zentral gegen diese Bedrohungen verteidigen können (siehe Abbildung 7). Vor allem müssen IT-Administratoren wissen, auf welche Weise Malware in ihre Netzwerke eindringt. Weitere Medien, die geschützt werden müssen, sind Instant Messaging und Kollaborations-Software.

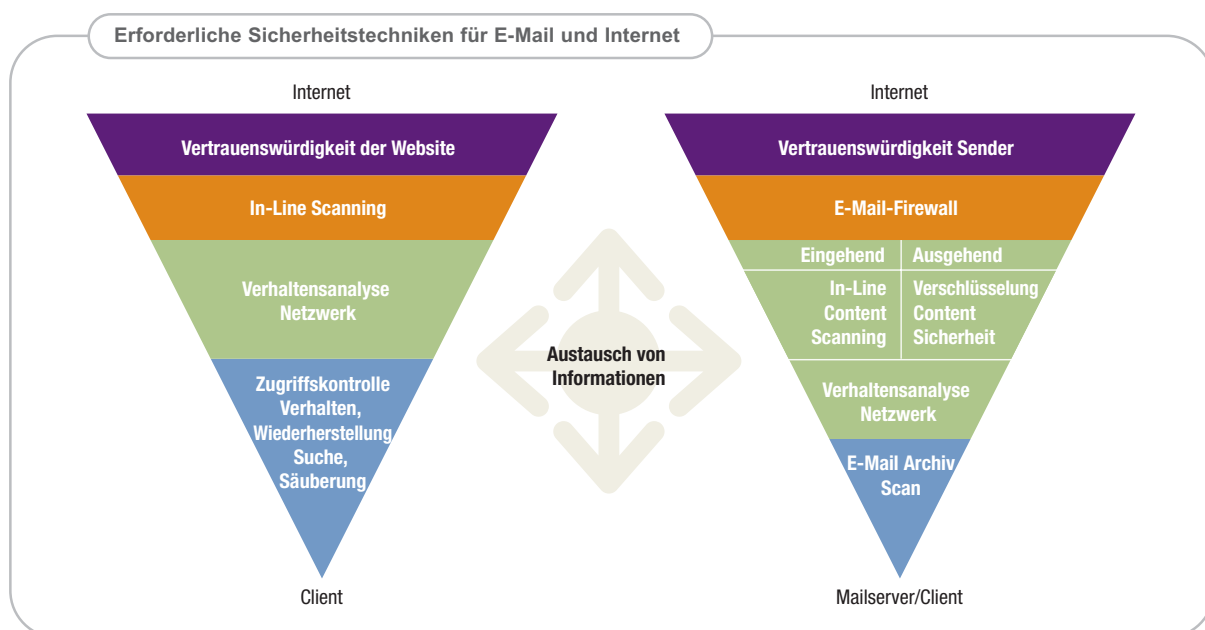


Abbildung 7. Trend Micro empfiehlt Lösungen, die einen Austausch zwischen den erforderlichen Sicherheitstechniken für E-Mail und Internet und die zentrale Verteidigung von Netzwerken gegen diese Bedrohungen ermöglichen.

FAZIT

Internet-Bedrohungen sind eine aktuelle Bedrohung, ihre Zahl und ihre Auswirkungen wachsen. Ihre Komplexität, ihr Variantenreichtum und die Verwendung mehrerer Übertragungswege, kombiniert mit der Tatsache, dass sie über das heutzutage am meisten genutzte Medium angreifen, verwandeln Internet-Bedrohungen in die größte Bedrohung, der sich Unternehmen, Dienstleister und Verbraucher seit langer Zeit gegenübersehen. Die Schäden infolge dieser Bedrohungen zeigen sich in Form des Verlusts vertraulicher Informationen, was Auswirkungen auf den Ruf der Marke, rechtliche und juristische Folgen und Schäden aufgrund des Verlusts von vertraulichen Informationen an Wettbewerber nach sich zieht. Da traditionelle Ansätze vor Internet-Bedrohungen keine Sicherheit bieten, befindet sich die Informationssicherheitsindustrie am Scheideweg. Unternehmen aller Größen und Dienstleister müssen Lösungen auf der Grundlage eines integrierten, mehrschichtigen Ansatzes entwickeln, der einen geeigneten Schutz vor diesen Bedrohungen bietet.

HERAUSFORDERUNGEN UND LÖSUNGEN: INTERNET-BEDROHUNGEN

LITERATURHINWEISE

1. IDC, Pressemitteilung, 18. Juli 2006, „Private Internet Use by Staff Threatens IT Security in Danish Companies, Says IDC,“ http://www.idc.com/getdoc.jsp?containerId=pr2006_07_14_125434.
2. Gregg Keizer, TechWeb Technology News, 24. Januar 2006, „Botnet Creator Pleads Guilty, Faces 25 Years,“ <http://www.techweb.com/wire/security/177103378>
3. Marius Oiaga, Softpedia, 4. Oktober 2006, „Hacking Russian Trio Gets 24 Years in Prison,“ <http://news.softpedia.com/news/Hacking-Russian-Trio-Gets-24-Years-in-Prison-37149.shtml>.
4. Byron Acohido und Jon Swartz, USA TODAY „Cybercrime flourishes in online hacker forums,“ 11. Oktober 2006, http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hacker-forums_x.htm
5. Consumer Reports (Verbraucherbericht), „Don't bite at phishers' e-mail bait,“ September 2006, http://www.consumerreports.org/cro/personal-finance/news/september-2006/dont-bite-at-phishers-e-mail-bait-9-06/overview/0609_dont-bite-at-phishers-email-bait_ov.htm.
6. Polizei der Stadt München, 25. August 2006, <http://www.sueddeutsche.de/tt3m3/muenchen/artikel/612/83529/>
7. „Scammers Hooking Bigger Phish,“ Asia.Internet, 9. November 2006, <http://asia.internet.com/news/article.php/3642971>.
8. Herman Singh, Standard Bank, „Next Generation Internet Fraud and Techniques to Combat This,“ BMI-T Annual Banking Forum, 19. Oktober 2006, Johannesburg, <http://www.bmi-t.co.za/presentations/bf/links/presentations/Herman%20Singh.pdf>.
9. Markus Jakobsson, Jacob Ratkiewicz, „Designing Ethical Phishing Experiments: A study of (ROT-13) rOnI query features,“ International World Wide Web Conference Committee, WWW 2006, 23.-26. Mai 2006, Edinburgh, Scotland, ACM 1-59593-323-9/06/0005, http://www.informatics.indiana.edu/markus/papers/ethical_phishing-jakobsson_ratkiewicz_06.pdf.
10. Tom Krazit, Cnet, „Two in three retail PCs are notebooks,“ 20. Dezember 2006, http://news.com.com/Two+in+three+retail+PCs+are+notebooks/2100-1044_3-6144921.html.

Trend Micro™

Trend Micro Incorporated leistet Pionierarbeit im Bereich Content-Security und bei der Bewältigung von Bedrohungen. Das 1988 gegründete Unternehmen bietet Privatpersonen und Unternehmen jeder Größe mehrfach ausgezeichnete Sicherheits-Software, -Hardware und -Services. Der Hauptsitz befindet sich in Tokyo. Trend Micro unterhält Niederlassungen in über 30 Ländern und vertreibt seine Produkte weltweit durch Corporate und Value-Added-Reseller und Dienstleister. Weitere Informationen und Testversionen der Trend Micro Produkte und Services finden Sie auf unserer Website unter www.trendmicro-europe.com.

Trend Micro Deutschland GmbH

Lise-Meitner-Straße 4
D-85716 Unterschleißheim
Gebührenfreie Hotline in den USA:
1+800-228-5651
Telefon: 1+408-257-1500
Fax: 1+408-257-2003
www.trendmicro-europe.com

