


A background image showing a laptop on a desk with a speedometer overlay. The speedometer has markings from 0.0 to 6.0 and a needle pointing towards 4.0.

Trend Micro OfficeScan 10 Endpunktsicherheit oder Der neue Ansatz

Bestandteil der Trend Micro Enterprise-Sicherheitslösungen 

-  Ein revolutionärer,
neuer Ansatz zur
Endpunktsicherheit
in Unternehmen

Ein Trend Micro Whitepaper | März 2009

I. DRASTISCHER ANSTIEG AN BEDROHUNGEN

Die Anzahl der Bedrohungen durch Cyber-Kriminelle wächst mit alarmierender Geschwindigkeit. Während 2007 noch 205 einmalige Bedrohungen pro Stunde verarbeitet wurden, waren es 2008 bereits 799 – ein sprunghafter Anstieg von fast 400 %. Diese Zahlen werden von TrendLabs belegt, dem globalen Netzwerk aus Forschungs- und Support-Zentren von Trend Micro, das rund um die Uhr Bedrohungen überwacht und Präventionsstrategien entwickelt. TrendLabs überwacht bereits seit mehreren Jahren die erstaunliche Zunahme einmaliger Malware-Exemplare pro Stunde mit Ergebnissen, die allen die Augen öffnen.

Diese Zunahme wurde durch die Entwicklung weit verbreiteter Geschäftsbefähiger verstärkt, wie z. B. universeller Internet-Zugriff und die Abhängigkeit vom Internet für unternehmenskritische Kommunikation. Um sich an einem immer häufiger verfügbaren Ziel zu bereichern, hat sich die Malware-Industrie zu einer raffinierten, gut organisierten und profitablen Branche entwickelt. Nirgends spürt man die Auswirkungen so stark wie an den Endpunkten.

Cyber-Kriminelle haben erkannt, dass herkömmliche Ansätze zur Endpunktsicherheit nicht mit dem extrem hohen Aufkommen an Bedrohungen Schritt halten können, und dadurch eine Sicherheitslücke entdeckt, die sie ausnutzen können. Unternehmen kämpfen mit immer aufwändigeren und häufigeren Pattern-Updates, und Benutzer verzweifeln allmählich an den stetig wachsenden Anforderungen der Sicherheitslösungen, die ihre Endpunkt-Ressourcen belasten. Diese Probleme summieren sich zu einer idealen Angriffsfläche für gezielte Bedrohungen und datenentwendende Malware.

Es ist an der Zeit, die Endpunktsicherheit zu überdenken und Annahmen bezüglich der Bereitstellung von Endpunktschutz zu hinterfragen. Häufigere Updates und aufwändigere Signaturen sind keine Antwort. IT-Administratoren wünschen sich sehnlichst, nicht mehr durch immer komplexere Endpunkt-Sicherheitslösungen eingeschränkt zu werden, die immer mehr Verwaltungsaufwand kosten. Endbenutzer möchten endlich wieder ungestört arbeiten können, ohne zu befürchten, dass ihre Endpunkt-Sicherheitslösung die begrenzten Prozessor- und Arbeitsspeicherressourcen ihrer Geräte mit Beschlag belegt.

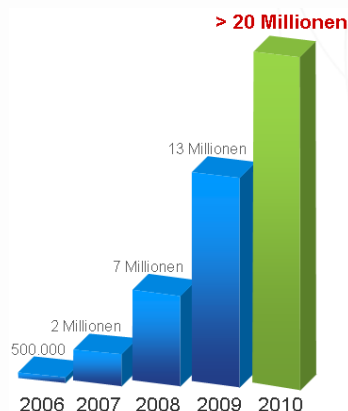


Abbildung 1: Der drastische Anstieg einmaliger Malware-Exemplare¹

Mit OfficeScan 10 stellt Trend Micro eine revolutionäre, neue Verteidigungsstrategie gegen das Aufkommen heutiger Bedrohungen vor: Die File-Reputation-Technologie entlastet den Endpunkt, indem sie ins Internet verlagert wird. Das vorliegende Whitepaper beschreibt diese neue Technologie und den damit verbundenen, wirksameren Schutz für Unternehmensendpunkte, während der Verwaltungsaufwand für Administratoren und die Ressourcenauslastung für Endbenutzer reduziert werden.

II. KOMPLEXITÄT ERHÖHT DIE SICHERHEITSRISIKEN

In den letzten Jahren gab es unter den Anbietern von Endpunkt-Sicherheitslösungen für Unternehmen einen regen Kampf um die besten Funktionen. Mit dem Auftreten neuer Bedrohungen wurden neue Funktionen zu ihrer Abwehr entweder erworben oder entwickelt. Da jede neue Technologie den Markt förmlich überrannte, war es für die meisten Anbieter schwierig, mit der daraus resultierenden, steigenden Anzahl an Neuerwerbungen Schritt zu halten. Dies führte zu ausufernden Produktangeboten. Doch auch wenn die Aufregung schon lange vorbei ist, bleibt die Frage: „Sind Unternehmensendpunkte sicherer geworden?“

Bei einer solchen Vielzahl an Einzellösungen und taktischen Funktionen sehen sich Unternehmen häufig mit der Komplexität ihrer Lösungen überfordert. Tatsächlich bereitet die Komplexität vieler herkömmlicher Lösungen den Unternehmen mehr Kopfzerbrechen als die Bedrohungen, die sie abwehren sollen.

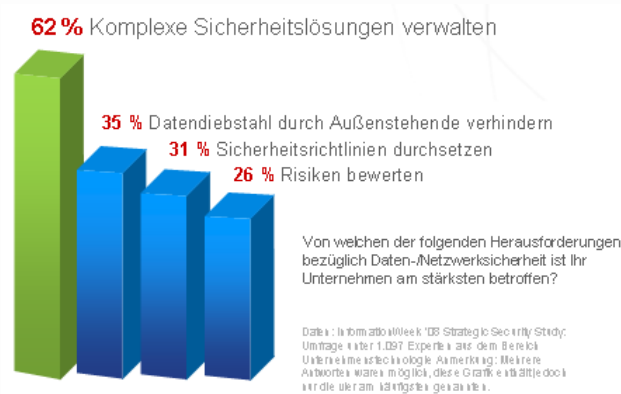


Abbildung 2: Die größten IT-Sicherheits Herausforderungen²

Bei vielen Unternehmen liegt die Komplexität der Endpunktsicherheit darin, täglich eine zunehmende Anzahl an Pattern-Datei-Updates zu verwalten und auf Tausende von Endpunkten zu verteilen. Faktoren wie die steigende Anzahl mobiler Endpunkte, komplexe Netzwerkinfrastrukturen und immer häufigere Pattern-Updates stellen die Sicherheit zunehmend auf die Probe – und machen die Wirksamkeit einer ansonsten starken Abwehr regelrecht zunichte.

Je mehr Bedrohungen abgewehrt werden müssen, desto mehr Endpunktressourcen werden dabei verbraucht und Endbenutzer immer mehr durch verringerte Rechenleistung belastet. Laut IDC haben Beschwerden von Unternehmen und Privatbenutzern zugenommen: „Die Sicherheitslösung frisst meinen Computer. Das Hochfahren dauert ewig. Suchläufe der Antiviren-Software machen das Arbeiten unmöglich. Sicherheitsmaßnahmen im Hintergrund verlangsamen Anwendungen und den Internet-Zugriff.“ Folglich sinkt die Produktivität von Endbenutzern, die entweder frustriert ihren nutzlosen Computer verlassen oder sich lieber damit beschäftigen, wie sie ihren Virenschutz deaktivieren können.

Trend Micro ist sich bewusst, dass Komplexität eine ebenso große Herausforderung wie der wirksame Schutz ist. Die Sicherheitslösungen von Trend Micro für Unternehmen sind daher darauf ausgerichtet, sofortigen Schutz bei weniger Aufwand zu erzielen. Andernfalls werden die Vorteile verbesserter Sicherheit durch die Produktivitätseinbußen zunichte gemacht. Der Ansatz von Trend Micro zur Endpunktsicherheit meistert diesen Balanceakt und macht ihn daher so einzigartig.

III. WARUM EIN NEUER ANSATZ?

Aktuelle Endpunktsicherheit beruht auf dateibasierter Bedrohungsabwehr mit Pattern (oder Definitionen), deren Updates regelmäßig und paketweise von den Sicherheitsanbietern auf die Endpunkte übertragen werden. Sobald die Sicherheitssoftware auf dem Computer ein neues Update erhält, wird ein neues Paket mit Pattern-Definitionen auf die Festplatte und den Speicher geladen. Bei jeder neuen Malware-Gefahr muss dieses Pattern erneut aktualisiert und auf den Benutzercomputer geladen werden, um permanenten Schutz zu gewährleisten. Die Zeit, die für das Update benötigt wird, bedeutet eine Sicherheitslücke für den Computer.

Da Angriffe immer schneller erfolgen, bildet das Aufkommen von Bedrohungen eine neue Art von Sicherheitsrisiko. Das konstante Aktualisieren kann die Leistung von Servern und Arbeitsstationen, die Nutzung der Netzwerkbandbreite sowie die kritische Zeitspanne beeinträchtigen, die zur Bereitstellung eines qualitativ hochwertigen Schutzes notwendig ist.

Um dieses extrem hohe Aufkommen von Bedrohungen wirksam zu bekämpfen, hat Trend Micro im Alleingang einen neuen Ansatz entwickelt, um sich gegen die vom Malware-Aufkommen ausgehende Bedrohung zu wappnen. Durch den Einsatz einer revolutionären, neuen Technologie und Architektur verlagert Trend Micro den Großteil der gespeicherten Malware-Signaturen vom Endpunkt ins Internet. Durch diese Entlastung bietet Trend Micro sofortigen Schutz vor einem auch zukünftig ständig wachsenden Aufkommen von Sicherheitsrisiken.

IV. FILE REPUTATION

Bei der herkömmlichen Malware-Suche werden infizierte Dateien entdeckt, indem mehrere Hash-Werte des Dateiinhalts mit einer Liste von Hash-Werten verglichen werden, die in einer Pattern-Datei gespeichert sind. Wenn eine Datei nach dem ersten Hash-Vergleich als verdächtig gekennzeichnet wird, verwendet die Scan Engine einen mehrphasigen Ansatz, um weitere Informationen zu ermitteln. In allen heute gebräuchlichen Endpunkt-Sicherheitslösungen wird diese Pattern-Datei auf dem Endpunkt gespeichert und muss regelmäßig verteilt werden, um vor den neuesten Bedrohungen schützen zu können.

Trend Micro bricht mit diesem Paradigma. Unsere neue File-Reputation-Technologie entkoppelt Pattern-Datei und lokale Scan Engine und führt Pattern-Dateiabgleiche mit einem intelligenten Suchserver über das Netzwerk durch. Dieser intelligente Suchserver kann sich am Kundenstandort oder auch im Internet befinden. Durch diesen webbasierten Ansatz ist es wesentlich einfacher, eine große Anzahl von Pattern-Dateien an Hunderte oder Tausende von Endpunkten zu verteilen. Mit diesem neuen Ansatz von Trend Micro werden die Suchkomponenten aller Clients, die diesen intelligenten Suchserver verwenden, sofort aktualisiert, sobald dort ein Pattern-Update vorliegt. File Reputation reagiert auf die heutigen Herausforderungen der Endpunktsicherheit von Unternehmen, da sie schneller und weniger aufwändig Schutz bietet.

„Trend Micro entlastet die Kundenendpunkte vom Aufwand der signaturbasierten Anti-Malware-Suche und überträgt diese in das Smart Protection Network. Dieser drastische Schritt hat seinen Ursprung in der Erkenntnis, dass der Versuch, Tausende von Angriffssignaturen täglich auf Millionen von Endpunkten in angemessener Zeit zu verteilen, kein brauchbarer Ansatz ist. Mit der innovativen Strategie von Trend Micro erweitert sich der Abwehrradius, so dass Angriffe auf Kundenendpunkte und Unternehmensnetzwerke schon im Vorfeld gestoppt werden.“

Ogren Group, August 2008

KOMPONENTEN DER ARCHITEKTUR

Webbasierter Client

Die zentrale Suchkomponente der Endpunkt-Sicherheitslösung von Trend Micro ist der webbasierte Client. Er ist zwar mit der Scan Engine für die herkömmlichen Überprüfung von Inhalten vergleichbar, arbeitet jedoch mit den intelligenten Suchservern zusammen, um mit Sicherheit feststellen zu können, ob eine Datei infiziert ist oder nicht, und welche Aktion durchgeführt werden soll.

Intelligenter Abfragefilter

Der intelligente Abfragefilter ist eine Komponente des webbasierten Clients und hindert diesen daran, wegen jeder einzelnen zu durchsuchenden Datei eine Abfrage an den Suchserver zu stellen. Der intelligente Abfragefilter verwendet komplexe mathematische Modelle, um mit einem hohen Grad an Präzision zu ermitteln, ob sich die durchsuchte Datei in der tatsächlichen Pattern-Datei befindet. Der intelligente Abfragefilter übersieht keine infizierten Dateien und erzeugt nur wenige Fehlalarme. Dies liegt hauptsächlich in seinen Funktionsprinzipien begründet. Wenn eine Datei vom intelligenten Abfragefilter nicht in die Weiße Liste aufgenommen wird, wird der Zwischenspeicher für die lokale Signatur abgefragt, um die Signatur für diese Datei zu suchen. Wenn das Netzwerk offline ist, also kein intelligenter Suchserver abgefragt werden kann, verweist der intelligente Abfragefilter auf einen „Index“ der Pattern-Datei, über den ermittelt werden kann, ob die jeweilige Datei sich NICHT in der Pattern-Datei auf dem intelligenten Suchserver befindet.



Abbildung 3: Ablaufdiagramm des Suchservers

Intelligenter Suchserver

Der intelligente Suchserver befindet sich im Kundennetzwerk, um einfachen Zugriff auf Endpunkte zu ermöglichen. Dadurch wird der Netzwerkverkehr am Gateway minimiert und die Latenzzeit webbasierter Pattern-Abgleiche reduziert. Der intelligente Suchserver speichert Pattern-Dateien von Trend Micro sofort nach Empfang. Bei Bedarf weist der intelligente Suchserver die intelligenten Abfragefilter des Clients auch auf Updates hin, die während der nächsten Anfrage des webbasierten Clients durchgeführt werden. Grundsätzlich ist der intelligente Suchserver die einzige Komponente der Lösung, die häufige Updates erhält. Es ist viel einfacher und bedeutend schneller, nur eine zentrale Komponente immer häufiger zu aktualisieren, als Pattern auf alle einzelnen Endpunkte zu verteilen.

V. ENDPUNKTSICHERHEIT ÜBERDENKEN

BEDROHUNGEN ÜBERDENKEN

In den letzten Monaten ist die Anzahl an Bedrohungen exponentiell gestiegen. Das Risiko, dass Unternehmen durch neue Malware bedroht sind, hat beträchtlich zugenommen. Während zentrale Orte, wie Gateways und Mail-Server, durch die immer häufigere Veröffentlichung von Pattern geschützt werden, gilt dies nicht für Unternehmensendpunkte. Die Sicherheitslücken einzelner Endpunkte zu schließen, ist schwierig, da häufigere Updates der Schutzkomponenten auf den Clients mit Zeit und Aufwand verbunden sind.

PATTERN-VERWALTUNG ÜBERDENKEN

Die Verwaltung von Pattern in verteilten Unternehmensumgebungen ist eine entscheidende Herausforderung für Sicherheitsadministratoren. Eine inkonsistente Pattern-Verteilung bedeutet nicht nur ein zusätzliches Risiko für einzelne Clients, sondern macht auch eine realistische Risikobewertung unmöglich. In Unternehmen jeder Größe bemühen sich Administratoren, auf allen Endpunkten die Aktualität der gleichen Pattern-Dateien zu garantieren. Erhöhte Mobilität und schnell aufeinander folgende Pattern-Veröffentlichungen erschweren jedoch die Abwehr von Bedrohungen. Malware-Schutz bedeutet heute nicht mehr, jede einzelne Bedrohung abzuwehren. Vielmehr ist es realistischer, mit Hilfe eines Pakets leistungsstarker Tools zur Risikobewältigung den bestmöglichen Schutz bereitzustellen.

Die Notwendigkeit, Pattern an Tausende oder Zehntausende einzelner Endpunkte zu verteilen, ist für Unternehmen mit einem hohen Aufwand verbunden. Es ist schwierig zu gewährleisten, dass alle Endpunkte – ob im lokalen Netzwerk oder als Roaming-Clients über das Internet – auf dem neuesten Stand sind. Und genau dies ist die Herausforderung, um ein gleiches Maß an Aktualität bezüglich Richtlinien und Pattern zu garantieren.

Die File-Reputation-Technologie bietet sofortigen, identischen Schutz an allen Endpunkten. Dadurch wird das gesamte Netzwerk schneller und konsistent geschützt und die Risikobewältigung vereinfacht. Dies reduziert die Komplexität bei der Verwaltung – und Bewältigung – einer stetig wachsende Anzahl an Pattern-Verteilungen und verbessert die Qualität des Schutzes.

ENDPUNKT-RESSOURCENVERBRAUCH ÜBERDENKEN

Das Speichern und Aktualisieren von Pattern-Dateien an den Endpunkten verbraucht erhebliche Ressourcen, insbesondere Arbeitsspeicher. Die heutigen, herkömmlichen Sicherheitslösungen können nur dann in Echtzeit und bei Zugriff Schutzfunktionen an den Endpunkten bieten, wenn sie auf Kernel-Ebene in das Betriebssystem integriert sind. Um bei Bedarf oder zeitgesteuert nach Bedrohungen zu suchen und diese leistungsstark und automatisch zu entfernen, muss jede einzelne Pattern-Datei nicht nur in den Kernel-Modus-Treiber, sondern auch in Benutzermodus-Komponenten geladen werden.

Trotz kontinuierlicher Optimierung des Dateiformats sind Pattern-Dateien in den vergangenen beiden Jahren erheblich größer geworden. Tatsächlich zeigt der Branchendurchschnitt der letzten Jahre eine

„Das Maß an Integration und Kooperation zwischen den verschiedenen Ebenen, Produkten und Services ist bei Trend Micro hoch entwickelt. Es wird zum Beispiel ein webbasierter Ansatz zur Bewältigung der Bedrohungen an den Endpunkten verwendet. Hierdurch wird die Systembelastung des Endpunktsicherheits-Clients reduziert. Die tatsächliche Lebensdauer älterer PCs, die den Ressourcenanforderungen neuer Sicherheitslösungen kaum nachkommen können, wird somit erweitert. Außerdem können Beschwerden von Benutzern an den Help-Desk reduziert werden, die sich mit der Verlangsamung der vorhandenen Hardware durch neue Sicherheitsprodukte befassen.“

IDC, August 2008

Erhöhung der Pattern-Dateigröße um 241 %³. Diese Tendenz wird sich in den kommenden Monaten fortsetzen, um sich gegen die unaufhaltsame Malware-Flut zu wappnen. Bei begrenzten Endpunkt-Ressourcen sind größere Pattern-Dateien auf Dauer einfach nicht tragbar. Das Konzept, Pattern-Dateien am Endpunkt zu speichern und zu aktualisieren, ist demnach früher oder später zum Scheitern verurteilt.

Die File-Reputation-Technologie von Trend Micro ist deutlich schlanker als herkömmliche Ansätze. Nur der Index des intelligenten Abfragefilters – sowie eine gelegentlich aktualisierte Pattern-Datei bei hochkomplexen Malware-Exemplaren – verbleibt auf dem Endpunkt. Durch die Verwendung webbasierter Pattern werden Ressourcen wieder für System und Anwendungen freigegeben, es steht mehr Arbeitsspeicher zur Verfügung, und die Gesamtleistung des Systems wird erhöht. Das Ergebnis: Verbessertes Benutzerkomfort und damit einhergehend eine Steigerung der Produktivität.

Letztendlich bedeutet dies, dass Endbenutzer, die keine bedeutenden Verzögerungen durch ihren Endpunktschutz bemerken, diesen mit höherer Wahrscheinlichkeit aktiviert lassen, was die Durchsetzung von Richtlinien vereinfacht. Endpunkte mit File Reputation verfügen eher über einen besseren und konsistenteren Schutz, da Endbenutzer sich nicht mehr veranlasst fühlen, die Endpunktsicherheit zu deaktivieren, um die Leistung zu beschleunigen. Da am Endpunkt weniger häufig und weniger aufwändig Signaturdateien heruntergeladen werden müssen, entlastet File Reputation die Endpunktressourcen und verbessert dadurch Leistung, Stabilität und Benutzerproduktivität.

File Reputation vereinfacht die Sicherheitsverwaltung bei gleichzeitiger Kosteneinsparung für das Unternehmen, da die netzwerkweite Implementierung rationalisiert wird. Dadurch kann Endpunktsicherheit auf jedem Computer unabhängig von Standort und Art der Verbindung erkannt und verwaltet werden. Mit weniger häufigen, leichteren Updates am Endpunkt entlastet File Reputation den Aufwand für die regelmäßige Verwaltung und Verteilung von Signaturdateien. Und da File Reputation die meisten Bedrohungen gemäß ihrer Vertrauenswürdigkeit an der Quelle abwehrt, sparen Administratoren Zeit und Kosten für die Säuberung der Endpunkte von Bedrohungen.

Darüber hinaus können mit File Reputation auch Gesamtkosten eingespart werden, da die Ressourcenauslastung vorhersehbar und dadurch verwaltbar wird. Beispielsweise werden sich die Systemvoraussetzungen für Endpunkte mit File Reputation in den nächsten Jahren auch dann nicht unerwartet erhöhen, wenn die Anzahl an Bedrohungen zunimmt. Unternehmen verfügen also stets über aktuellem Schutz, ohne ihre Endpunkte ungeplant aktualisieren zu müssen.

ANFORDERUNGEN AN DIE BANDBREITE ÜBERDENKEN

Die Verteilung von Pattern an eine Vielzahl von Endpunkten erfordert große Mengen an Netzwerkbandbreite, die mit immer schnelleren Pattern-Veröffentlichungen stetig anwächst. Um zu beurteilen, wie viel Bandbreite durch File Reputation eingespart werden kann, ist zu beachten, dass gleiche Aktualität der Schutzkomponenten – insbesondere in der kürzestmöglichen Zeit – nur erreicht werden kann, wenn Patterns erheblich schneller und häufiger als heute auf einzelne Endpunkte verteilt werden. File Reputation erreicht diese relative Geschwindigkeit, indem die Pattern-Datei nur einmal übertragen wird, und zwar an den intelligenten Suchserver. Dies spart ungeheuer viel Netzverkehr, der andernfalls für die Verteilung desselben Patterns an Tausende von Endpunkten erforderlich gewesen wäre.

VI. PROFITIEREN AUCH SIE VON DIESER REVOLUTIONÄREN ENDPUNKTSICHERHEIT!

OfficeScan 10 ist für mittelständische und große Unternehmen die richtige Wahl. Die revolutionäre File-Reputation-Technologie entlastet Ihre Endpunkt-Ressourcen und verringert den Aufwand für Verwaltung und Verteilung einer ständig zunehmenden Anzahl an Pattern-Dateien. Unabhängig vom Standort Ihrer Endpunkte – ob am Flughafen, im Hotel, im Home Office oder innerhalb Ihres Unternehmensnetzwerks – werden sie sofort bei weniger Aufwand geschützt.

Erfahren Sie, wie Sie Ihre Endpunktsicherheit neu überdenken können.

<http://de.trendmicro.com/de/solutions/enterprise/security-solutions/endpoint-security/>.

¹ AV-Test. „Erheblich mehr Viren, Würmer und andere Malware als jemals zuvor.“ Datenerfassung durch Andreas Marx (aufgeführt in Artikeln im Nachrichtenarchiv von AV-Test, 11. Januar 2008).

Quelle: <http://www.av-test.org/index.php?menue=2&sub=Newsarchiv&lang=0>

² InformationWeek Analytics. „2008 InformationWeek Strategic Security Survey.“ Mike Fratto. Juni 2008.

³ Interne Vergleichstests von Trend Micro.

© 2009 by Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro T-Ball-Logo, OfficeScan und TrendLabs sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- und/oder Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. [WP03_FileReputation_090305DE]