

Whitepaper

Angriffsziel Endpoint

KASPERSKY Lab

**SOLID
BUSINESS
PROTECTION**
BUILT THE RIGHT WAY

www.kaspersky.de

Inhaltsverzeichnis

▶ Der Kampf um den Endpoint.....	3
▶ Die wachsende Bedrohung durch Malware.....	4
▶ Warum wird der Endpunkt zum Ziel?.....	6
▶ Wie greifen Cyberkriminelle Endpoints an?.....	8
▶ Endpoints vor Cyberkriminalität schützen.....	10
▶ Ein typisches Beispiel – Sind Sie wirklich sicher?.....	12

Der Kampf um den Endpoint

Ende 2009 brachten Cyberkriminelle die Banking-Anmeldedaten – also Benutzername und Kennwort – der in Plano in Texas ansässigen Hillary Machinery Inc. in ihren Besitz und nahmen innerhalb von drei Tagen mehr als 45 separate Überweisungen an über 40 verschiedene Zahlungsempfänger vor. Das Ergebnis war ein Verlust von 801.495 US-Dollar. Hillary Machinery konnte zwar einen Teil des verlorenen Geldes zurückerlangen. Es blieben jedoch 250.000 US-Dollar plus Anwaltsgebühren und Gerichtskosten offen, während das Unternehmen gleichzeitig einen Prozess gegen seine Bank anstrebte, der bis heute andauert. Firmeninhaber Troy Owen dazu: „Der Verlust hat zwar nicht dazu geführt, dass wir unser Geschäft aufgeben mussten. Er hat jedoch mit Sicherheit die Wachstumspläne vereitelt, die wir für das Unternehmen hatten.“

Wenn Sie an einem beliebigen Tag eine Zeitung aufschlagen, finden Sie Berichte über Unternehmen, die von Cyberkriminellen attackiert wurden. Verletzungen der Datensicherheit greifen immer mehr um sich. Banking-Trojaner stehlen Anmeldedaten für das Online-Banking und verursachen so enorme finanzielle Schäden. Im Jahr 2010 führte das CSO Magazine eine Umfrage zur Cybersicherheit durch (Cyber Security Watch Survey). Chefredakteur Bill Brenner stellt fest: „Selbst Unternehmen, die erheblichen Aufwand zum Schutz ihrer Daten betreiben, räumen ein, dass man den Kriminellen kaum entgehen kann.“

Was hier vorgeht, ist nichts Geringeres als eine Schlacht – ein Kampf gegen Cyberkriminelle, die nur ein Ziel haben: sich Geld zu erschleichen. Die heutigen Cyberkriminellen sind unentwegt auf der Suche nach Daten, mit denen sich leicht Profit machen lässt, sowie Anmeldedaten, mit denen sie direkt Geld von Unternehmenskonten abbuchen können.

Der Bericht „The Top Cyber Security Risks“ von SANS.org stellt fest: „Die Zahl der Angriffe ist mittlerweile so groß, und die Methoden der Kriminellen sind inzwischen so ausgefeilt, dass es vielen Unternehmen Schwierigkeiten bereitet, zu erkennen, welche neuen Gefahren und Schwachstellen das größte Risiko darstellen, und wie Ressourcen eingesetzt werden müssen, um die Angriffe mit der höchsten Wahrscheinlichkeit und dem größten Schadenspotenzial zuerst zu bekämpfen.“ Wenn IT-Abteilungen in Sicherheit investieren, übersehen viele das Hauptangriffsziel – den Endpoint.

Der Endpoint – der Desktop, Laptop oder das Mobilgerät eines Benutzers – ist für Cyberkriminelle heute das lohnendste Ziel. Die Endpunktsysteme werden immer mobiler, wodurch der herkömmliche IT-Schutzbereich wirkungslos wird, wenn es darum geht, das richtige Schutzniveau für Unternehmensanwender und -ressourcen zu gewährleisten. Laut IDC sind „Endpoint-Lösungen inzwischen eine Hauptverteidigungslinie.“

Der vorliegende Artikel erörtert die wachsende Bedrohung durch Malware und erläutert, auf welche Weise Cyberkriminelle Endpoints angreifen, und wie Sie Endpoints vor solchen Angriffen schützen können.

Die wachsende Bedrohung durch Malware

Kaspersky Lab arbeitet seit über 14 Jahren am Schutz von Unternehmen vor den Gefahren des Internets. In dieser Zeit haben wir ein exponentielles Wachstum der Bedrohungen durch Viren im heutigen Internet beobachtet. Die Zahlen sind ernüchternd. Täglich werden über 30.000 neue Bedrohungen entdeckt – mehr als 3,4 Millionen allein im Jahr 2009. Jeden Tag werden über 3.500 neue Virensignaturen veröffentlicht, um den Schutz vor den neuesten Bedrohungen sicherzustellen. An einem besonders geschäftigen Tag hat Kaspersky Lab 13.500 Signaturen erstellt, um die hohe Anzahl der an diesem Tag erkannten Bedrohungen zu bekämpfen. Neben dem traditionellen Schutz von Workstations und Servern wurden über 1.200 Virensignaturen für Mobilgeräte erstellt, um Smartphones vor Bedrohungen zu schützen.

Der Trend setzt sich im Jahr 2010 fort:

- Im ersten Quartal 2010 wurde über 327 Millionen mal versucht, Computer auf der ganzen Welt zu infizieren – eine Steigerung von 26,8 Prozent gegenüber dem vorherigen Quartal.
- Weiterhin wurden im ersten Quartal 2010 mehr als 119 Millionen Server entdeckt, auf denen Malware gehostet wurde. Dabei befanden sich 27,57 Prozent der Server in den USA, 22,59 Prozent in Russland und nur 12,84 Prozent in China.
- Die Gesamtzahl der Angriffe auf Schwachstellen in Browsern und Plugins sowie in PDF-Betrachtern stieg um 21,3 Prozent, und fast die Hälfte dieser Angriffe richtete sich gegen Schwachstellen in Adobe-Programmen.

Ein kürzlich von RSA veröffentlichtes Whitepaper zum Thema Cyberkriminalität enthüllt, dass 88 Prozent der Fortune-500-Unternehmen kompromittierte PCs in ihren Umgebungen betreiben, die mit Trojanern infiziert sind. Laut Uri Rivner von RSA „sind diese Trojaner damit beschäftigt, Terabyte an Unternehmensdaten zu getarnten Abwurfzonen zu befördern, die über die gesamte „Dunkle Cloud“ der kriminellen Infrastruktur verstreut sind.“ Dies stimmt mit den von CNET News im Oktober 2009 gemeldeten Daten überein, denen zufolge 63 Prozent aller mittleren Unternehmen einen Anstieg der Cyberbedrohungen im Jahr 2009 registrierten. Laut diesem Artikel sind 71 Prozent der in den USA ansässigen mittleren Unternehmen der Auffassung, dass sie ein ernsthafter Einbruch in den Ruin treiben könnte. Diese alarmierende Einschätzung belegt einmal mehr das Hauptziel heutiger Cyberkriminalität – Geld abzugreifen. Tatsächlich haben laut dem Internet Crime Complaint Center des FBI die angezeigten Straftaten im Jahr 2009 um 22,3 Prozent zugenommen.

Die Schäden, die durch Cyberkriminalität verursacht wurden, haben sich jedoch im gleichen Jahr von 265 Millionen US-Dollar auf 560 Millionen mehr als verdoppelt. Und diese Zahlen beinhalten nur diejenigen Angriffe, die gemeldet wurden. Da der größte Teil aller Angriffe nicht zur Anzeige gebracht wird, sind die Zahl der Angriffe und die finanziellen Verluste tatsächlich noch deutlich höher.

Zusätzlich zu den ausgefeilteren Angriffsmethoden, die zu größeren gestohlenen Geldbeträgen pro Einbruch führen, greifen Cyberkriminelle inzwischen auch nicht mehr nur Großunternehmen an. Kleine Unternehmen, staatliche und kommunale Behörden sowie Bildungseinrichtungen werden gezielt von Cyberkriminellen angegriffen, weil diese oftmals nur wenig in Sicherheit und Schutz investieren. Mittlere Unternehmen in den USA haben im Jahr 2009 über 100 Millionen US-Dollar durch betrügerische Banküberweisungen verloren. Selbst das Pentagon – eine Behörde mit enormen Investitionen in Sicherheit – wurde 2009 Opfer von Cyberkriminellen, was zum Verlust von Terabyte sensibler Daten führte, darunter auch Daten zum neuen Kampfflugzeug F35 Lightning II Joint Strike.

Während im Verteidigungsministerium die Daten mit der höchsten Vertraulichkeitsstufe auf Computern gespeichert werden, die nicht mit dem Internet verbunden sind, haben Hacker über Endpunkt-Computer von Drittunternehmen, die mit dem Entwurf und Bau der Kampfflugzeuge beauftragt wurden, Zugang zu diesen hochsensiblen Daten erlangt.

Warum wird der Endpunkt zum Ziel?

Die wachsende Bedrohung durch Viren konzentriert sich heutzutage auf ein Ziel – den Endpunkt. Warum ist das der Fall? Weshalb haben Cyberkriminelle so großes Interesse am Endpunkt entwickelt? Der Endpunkt ist aus vielen Gründen für Cyberkriminelle interessant:

- **Dezentrale Daten.** Die Daten werden nicht länger auf Zentralrechnern abgelegt. Ständig werden sensible und vertrauliche Unternehmensdaten auf Desktops, Laptops und Mobilgeräten erstellt, verwendet und gespeichert. Der Zugang zu diesen Geräten bedeutet Zugriff auf Daten, die möglicherweise einen hohen finanziellen Wert haben.
- **Der Schlüssel zur Schatztruhe.** Wenn ein Cyberkrimineller auf einem Endpunktsystem den richtigen Trojaner platziert, erhält er unter anderem Zugriff auf Anmeldedaten für weitere Unternehmenssysteme – einschließlich Online-Banking und Finanzsysteme. Mittels der von Trojanern erbeuteten Anmeldedaten werden jeden Tag Millionenbeträge durch betrügerische Überweisungen von Unternehmenskonten entwendet.
- **Vollständige Kontrolle.** Durch umfassenden Zugriff auf Administratorebene am Endpunkt erhalten Cyberkriminelle Zugang zu allen Systemen und Daten, auf die der Endanwender Zugriff hat. Zusätzlich hat der Cyberkriminelle die Möglichkeit, den Endpunkt in einen „Zombie“-Computer zu verwandeln, der Teil eines umfassenderen Botnetzes ist und zur Verbreitung von Malware auf anderen Computern genutzt wird. Und schließlich erhalten Hacker durch diese Art von Endpunkt-Zugang die Möglichkeit, E-Mails, IM-Kommunikation, Webdatenverkehr, einzelne Tastatureingaben und vieles mehr mitzulesen, wodurch der Endpunkt zu einer wahren Schatzgrube an Möglichkeiten wird.

Die Computer-Hacker von heute sind nicht die „Script-Kiddies“ von gestern, die nach öffentlicher Anerkennung streben. Die Cyberkriminellen der heutigen Zeit versuchen, Zugang zum Endpunkt zu erlangen und gleichzeitig verborgen zu bleiben, sodass sie ohne Wissen des Benutzers Daten und Geld entwenden können.

Es gibt eine Reihe von Faktoren, welche den Endpunkt zu einem leichten Ziel machen:

- **Einfacher Zugang.** Durch neue Applikationen und Web 2.0 müssen auch Unternehmen ihren Mitarbeitern den Zugriff auf alle Möglichkeiten des Internets gestatten. Damit wird der Endpoint zum neuen Ziel für Cyberkriminelle.
- **Mobile Daten.** Mobile Außendienstmitarbeiter reisen tagtäglich um die Welt und stellen Verbindungen zu unsicheren Netzwerken auf Flughäfen, in Hotels, zu Hause oder in Flugzeugen her. Da diese Systeme außerhalb der Grenzen des Unternehmensnetzwerks liegen, stellen sie ein permanentes Risiko für Unternehmensdaten dar und machen den Perimeter noch durchlässiger und anfälliger für Cyberkriminalität.
- **Mehrere Angriffsvektoren.** Endanwender nutzen das Internet im Unternehmen heutzutage sowohl für geschäftliche als auch für private Zwecke, was Cyberkriminellen mehrere Einfallstore öffnet.

Legitime geschäftliche Webseiten werden zu Virenverteilern und Soziale Netzwerke zur Spielwiese für Cyberkriminelle. Cyberkriminelle machen gleichermaßen Jagd auf Einzelpersonen und Unternehmen, während diese sich in Sozialen Netzwerken bewegen, um den Kontakt zu Freunden, der Familie, Kunden, Interessenten und Partnern zu halten. Das private Surfen im Internet sowie Dating-, Musik- und Video-Portale liefern ebenfalls Angriffsmöglichkeiten für Cyberkriminelle, über die sie Endpoints mit Malware infizieren. Nicht zu vergessen ist auch die immerwährende Gefahr, die von E-Mails ausgeht.

Das Endziel besteht darin, Malware auf den Endpunkt zu befördern. Noch einmal die RSA:

„Malware, bei der es sich meist um Trojaner handelt, beginnt nach der Infektion damit, sämtlichen internetbezogenen Datenverkehr aufzuzeichnen, die Tastatureingaben des Benutzers mitzuschneiden sowie E-Mails, im Browser gespeicherte Kennwörter und eine Reihe weiterer Dinge zu entwenden. Der Trojaner macht bei den Anmeldedaten für das Online-Banking und Kreditkartendaten nicht Halt:

Er stiehlt Nachrichten in Sozialen Netzwerken, medizinische Daten, private Chat-Sitzungen, Wählerbriefe und sämtliche arbeitsbezogenen Inhalte: Anmeldedaten für interne Systeme, E-Mails, die Sie gesendet oder empfangen haben, Finanzergebnisse des Unternehmens und vertrauliche kundenbezogene Webformulare, die Sie in CRM-Systemen ausgefüllt haben.“

Wenn der Trojaner einmal auf dem Endpunkt installiert ist, kann er produktiv und heimtückisch werden – und auf vielfältige Weise unglaublich profitabel. Daher ist es weder ein Wunder noch ein Zufall, dass Cyberkriminelle den Endpunkt angreifen. Ohne den richtigen Schutz stellen die Endpoints von Unternehmen ein umfassendes Ziel mit einer großen Zahl von Einstiegspunkten dar.

Wie greifen Cyberkriminelle Endpoints an?

Kein Grund zur Sorge, glauben Sie? Denken Sie noch einmal darüber nach. Am Perimeter orientierte Sicherheitskonzepte sind wirkungslos, wenn es um den Schutz des neuesten Ziels der Cyberkriminellen geht. Laut Uri Rivner von RSA „... verändert sich das Schlachtfeld.

Mittlerweile stehen nicht mehr Netzwerke, sondern die Mitarbeiter in der Schusslinie.“ Betrachten wir daher, auf welche Weise Cyberkriminelle den Endpunkt angreifen. In den vergangenen Jahren war das Betriebssystem – hauptsächlich Microsoft Windows – das Paradies der Hacker. Mit zunehmender Sicherheit des Betriebssystems wurden Client-seitige Anwendungen auf den Endpoints zum bevorzugten Angriffsweg für Cyberkriminelle. Der Anwender lädt Anwendungen wie WinZip, Realplayer, Quicktime, Adobe PDF und Browser-Plugins (ActiveX-Steuererelemente, Video-Codex und so weiter) herunter, ohne sich Gedanken um die Wartung all dieser Anwendungen zu machen. Diese nicht dokumentierten und nicht verwalteten Programme, die voller Schwachstellen sind, werden selten ausgebessert oder aktualisiert. IT-Abteilungen wissen nur in den seltensten Fällen, welche Versionen dieser Anwendungen in ihren Umgebungen ausgeführt werden, ganz zu schweigen davon, welche Patches für diese Anwendungen installiert wurden.

Laut den Statistiken von Secunia PSI sind nur zwei Prozent aller Windows-Computer vollständig aktualisiert. Es sind diese Schwachstellen, über die Cyberkriminelle Zugang zu den Endpoints von Unternehmen erlangen und Malware einschleusen, um ihre üblen Machenschaften zu betreiben.

Cyberkriminelle nutzen eine Reihe von Angriffswegen, um den Endpunkt mit Malware anzugreifen:

- **Der Kommunikationsbedarf.** Gegenwärtig enthalten acht von zehn E-Mails schädliche oder unerwünschte Inhalte. Laut Gartner ist die Gefahr durch E-Mails im Jahr 2009 auf das Sechsfache angewachsen. Diese Zahl umfasst infizierte Anhänge, Phishing-Links und Umleitungen auf Server von Dritten, die Malware verteilen.
- **Kompromittierte Webseiten.** Über 1,73 Milliarden Anwender – das sind 25 Prozent der Weltbevölkerung – besuchen täglich mehr als 234 Millionen Webseiten. Allein 2009 wurden 47 Millionen neue Webseiten ins Internet gestellt. Cyberkriminelle nutzen die exponentielle Zunahme des Surfens im Internet, um arglosen Anwendern Malware unterzuschieben. Zwei Techniken, SQL-Injektionen und Cross-Site-Scripting, sind für 80 Prozent aller erfolgreichen Internetangriffe verantwortlich. Cyberkriminelle nutzen Schwachstellen im Internet aus, um sich in legitime Unternehmenswebseiten zu hacken und dort verschleierte JavaScript-Code zu platzieren, der Malware auf die Computer von Anwendern herunterlädt, welche die Webseite besuchen. Bei derartigen auch als „Drive-by-Download“ bezeichneten Angriffen kommen Anwender durch den bloßen Besuch legitimer Webseiten, die durch Server von Dritten kompromittiert wurden, mit Malware in Kontakt. Malware wird nicht länger ausschließlich über Glücksspiel- und pornografische Webseiten verteilt. Mittlerweile handelt es sich bei 77 Prozent der Webseiten, die schädliche Inhalte enthalten, um völlig legitime Webseiten, die von Cyberkriminellen kompromittiert wurden.

- **In Verbindung bleiben.** Soziale Netzwerke sind bei Einzelpersonen und Unternehmen gleichermaßen im Kommen. Das Bedürfnis, mit Partnern, Kunden, Interessenten, Familienmitgliedern und Freunden in Kontakt zu bleiben, hat die Unternehmen dazu bewogen, ihren Perimeterschutz für eine sehr unsichere Form der Massenkommunikation zu öffnen. Facebook, LinkedIn, Twitter und MySpace sind die wichtigsten Social-Media-Webseiten, die Unternehmen für den alltäglichen Zugriff durch ihre Mitarbeiter freigeben – sei es zu privaten oder geschäftlichen Zwecken. Cyberkriminelle nehmen die rapide ansteigende Nutzung von Sozialen Netzwerken ins Visier, um Geld abzugreifen sowie Malware auf Desktops und in Unternehmensnetzwerken zu verteilen.

Fallen in Sozialen Netzwerken machen sich zwei menschliche Grundeigenschaften zunutze: Vertrauen und Neugier. Der Vertrauensfaktor kommt dadurch zustande, dass Sie nur Personen einladen, die Sie kennen, denen Sie vertrauen und daher die von ihnen übermittelten Inhalte als „sauber“ einstufen. Die Neugier treibt unser Bedürfnis zu klicken. Der typische Anwender klickt praktisch alles an. Das Problem dabei besteht darin, dass wir nur selten wissen, wohin ein Link führt, oder welche Schäden durch das Öffnen der jeweiligen Datei, Webseite oder Anwendung entstehen können. Es ist die Kombination dieser bei den Faktoren, die Soziale Netzwerke außerordentlich gefährlich macht.

- **Angst, Unsicherheit und Zweifel (Fear, Uncertainty and Doubt, FUD).** Scareware und Ransomware werden immer häufiger genutzt, um arglosen und unerfahrenen Anwendern Geld abzunehmen. Beim Besuch einer Webseite wird eine Popup-Nachricht angezeigt, die den Anwender darüber informiert, dass sein System mit Malware infiziert und gefährdet ist. Gleichzeitig wird in der Meldung als Schutz falsche Sicherheitssoftware zum Download angeboten, die zwischen 30 und 60 US-Dollar kostet. Der Schutz dient dabei als Lockmittel. Tatsächlich haben Sie dabei jedoch Geld verloren, und die heruntergeladene Software ist in Wirklichkeit selbst Malware und kein Programm, das Sie vor Malware schützt. Geschickte Scareware-Betrüger erzielen wöchentliche Einnahmen, die mehr als das Dreifache des Einkommens betragen, das der Geschäftsführer so machen Unternehmens erhält.

Endpoints vor Cyberkriminalität schützen

Obwohl die Gefahr durch Malware exponentiell zunimmt, ist das Budget für IT-Sicherheit nicht in gleichem Maße erhöht worden. Vor allem haben die Investitionen in den Schutz der Endpoints nicht im gleichen Umfang wie die tatsächlichen Gefahren zugenommen. IT-Abteilungen konzentrieren ihre Ausgaben für Sicherheit traditionell auf den Perimeter – Firewalls, IDS, IPS, Spam-Module und URL-Filterung. Obgleich diese Ausgaben unbedingt notwendig sind und ein Schlüsselement jeder mehrstufigen Schutzstrategie darstellen, tragen sie kaum dazu bei, den Endpunkt vor dem Malware-Ansturm aus verschiedenen Richtungen zu schützen. URL-Filter verhindern zwar, dass Mitarbeiter Webseiten besuchen, die als schädlich eingestuft werden, bieten den Anwendern aber überhaupt keinen Schutz vor Malware, die per Drive-by-Download von legitimen Webseiten verteilt wird. Firewalls werden so konfiguriert, dass Anwender unbegrenzten Zugang zum Internet haben. Ironischerweise wurde Cyberkriminellen gerade dadurch der direkte Zugriff auf Desktops ermöglicht.

Der Schutz des Endpunkts wurde lange Zeit als Massenartikel angesehen, bei dem letztlich der Preis den Ausschlag gab. Einige Unternehmen setzen sogar kostenlose Antiviren-Software ein. Unglücklicherweise wird bei manchen Lösungen Malware kostenlos mitgeliefert. IT-Abteilungen konzentrieren sich auf den Schutz am Perimeter und schenken dem AV-Schutz kaum Beachtung. Einige IT-Manager sehen nur geringe Unterschiede zwischen den verschiedenen AV-Produkten. Andere halten Antiviren-Software generell für wenig sinnvoll und wählen diejenige Software aus, die scheinbar den niedrigsten finanziellen Aufwand bedeutet. Eine willkürlich oder nach niedrigstem finanziellen Aufwand ausgewählte Software bereitet nicht zwingend die wenigsten Probleme, eher im Gegenteil.

Diese Standpunkte sind zwar nachvollziehbar, angesichts der katastrophalen Erfahrungen einiger Kunden aber kaum zutreffend. Tatsächlich bestehen gravierende Unterschiede in der Art und Weise, wie AV-Software Malware auf dem Endpunkt erkennt und entfernt, was von zahlreichen unabhängigen Testlaboren immer wieder bestätigt wird. Die Zeit ist reif, aus diesem Denkmuster auszubrechen und sowohl die Erkennung als auch die Reaktion am Endpunkt in den Mittelpunkt der Betrachtung zu rücken.

Bei der Evaluierung von Lösungen für den Schutz von Endpoints ist eine Vielzahl von Faktoren zu berücksichtigen:

- **Gesamterkennungsrate:** Wie effektiv arbeitet der Anbieter bei der Erkennung sowohl bekannter als auch unbekannter Malware, wobei Ersteres auf signaturgestützten Analysen beruht und Letzteres durch heuristische oder regelgestützte Analysen realisiert wird? Der Anbieter sollte in der Lage sein, die verschiedenen Arten von Malware zu erkennen: Trojaner, Viren, Rootkits und mehr. Gute Ergebnisse bei einer Art der Erkennung in Verbindung mit schwachen Ergebnissen bei anderen Analysearten ergeben ineffektiven Schutz.
- **Ganzheitlicher Schutz:** Malware kann auf den verschiedenen Wegen auf einen Endpunkt gelangen, und jeder Anbieter von Antiviren-Software, der sein Geld wert ist, muss in der Lage sein, alle Angriffswege am Endpunkt zu blockieren. Zusätzlich muss der Anbieter in der Lage sein, das System unabhängig von seinem physischen Standort zu schützen und sich schnell auf wechselnde Standorte einstellen, damit auch beim Betrieb außerhalb der Grenzen des Unternehmensnetzwerks optimale Sicherheit gewährleistet ist. Personal Firewalls, IDs, Spam-, Viren-, Phishing- und Internetvirenschutz und so weiter sollten als grundlegende Bausteine einer umfassenden Strategie zum Schutz von Endpoints betrachtet werden.

- **Performance:** Der beste Schutz nützt wenig, wenn er den Anwender bei seiner täglichen Arbeit behindert. „Bloatware“, wie AV-Software häufig genannt wird, nimmt dermaßen viele Systemressourcen in Anspruch, dass Mitarbeiter ihr System nicht sinnvoll nutzen können, bis die Software die Überprüfung abgeschlossen hat. Daher ist es besonders wichtig, einen Schutz einzusetzen, der praktisch keine Auswirkungen auf die Produktivität der Mitarbeiter hat. Aber ist es überhaupt möglich, Schutz und Performance in einem Produkt zu vereinen? Die Antwort ist ein klares Ja!
- **Handhabung:** Die Verwaltungskonsole von Antiviren-Software ist ein besonders wichtiger Baustein – und ein entscheidendes Kaufkriterium. Eine schwerfällige, nicht einfach zu bedienende und ressourcenhungrige Verwaltungskonsole erschwert die Verwaltung des Sicherheitssystems und beeinträchtigt so die gesamte Sicherheitsstrategie. Die Verwaltung muss simpel, einfach zu bedienen, trotzdem fein abgestuft und leistungsfähig genug sein, um die Risiken an jeder Stelle der Endpunkt-Umgebung minimieren zu können. Und sie muss besonders bei der schnellen Bereitstellung und Aktualisierung der vielen Instanzen der Endpunkt-Sicherheit gute Unterstützung bieten.
- **Support:** Niemand hat die Zeit, seine Arbeit für 45 Minuten oder mehr zu unterbrechen und auf Hilfe zu warten, wenn ein Problem auftaucht – und Sie sollten auch nicht warten müssen. Testen Sie vor dem Erwerb eines AV-Schutzes das Supportzentrum, um sicherzugehen, dass es schnell und effektiv reagiert. Wie schnell werden Telefonanrufe angenommen? Wie effektiv arbeitet der Techniker bei der Lösung Ihres Problems? Der Support sollte keine Qual, sondern ein Pluspunkt sein.
- **Preis:** Dieser Aspekt wird aus einem bestimmten Grund zuletzt genannt: Heutzutage bieten alle AV-Anbieter sehr wettbewerbsfähige Preise. Hinsichtlich der Funktion sind jedoch nicht alle wettbewerbsfähig. Der Preis spielt zwar eine Rolle, aber erst dann, wenn Sie die Sicherheitssoftware mit dem richtigen Schutz, der richtigen Performance und der richtigen Handhabung gefunden haben.

Der Endpunkt-Schutz sollte nicht wie ein beliebiger Massenartikel erworben werden. Durch eine sorgfältige Prüfung können Sie sicherstellen, dass der Schutz Ihrer Endpoints den höchsten Ansprüchen an Erkennung und Reaktionsfähigkeit genügt.

Ein typisches Beispiel – Sind Sie wirklich sicher?

Herr Stephan, Administrator der öffentlichen Schulen von Jackson in Mississippi, war überzeugt, die richtigen Schutzvorkehrungen getroffen zu haben, um das Netzwerk frei von Viren zu halten. Angesichts der über 9.200 verwalteten Arbeitsplätze hatte Herr Stephan eine substanzielle Investition getätigt, um ihre Sicherheit zu gewährleisten. Als aufgrund von Performance-Problemen schließlich der Umstieg auf Kaspersky Lab erfolgte, fand man heraus, wie unsicher sie tatsächlich gewesen waren.

Bei der Installation der Kaspersky-Lösung stellte das IT-Team fest, dass weite Teile des Netzwerks von Viren befallen waren. Auf den Endpunkt-Systemen wurden gefunden:

- 14.459 Virenvorkommen
- 43 verschiedene Trojaner
- 56 verschiedene Viren
- 15.701 infizierte Objekte im gesamten Netzwerk

Die Malware war außer Rand und Band! Der aktuelle Anbieter war nicht in der Lage, die Malware zu erkennen und zu entfernen. Nur durch die Installation eines optimalen Malware-Schutzes wurde die Lage erkannt – dank Kaspersky Lab.

Angesichts der Investition, die die Einrichtung zum Schutz vor Risiken getätigt hatte, war die Infektionsrate unentschuldig. Es kostete mehrere Wochen mühevoller Arbeit, bis endlich sämtliche Viren-Infektionen im gesamten Netzwerk beseitigt waren. Sie glauben vielleicht, dass Sie sicher sind. Aber wissen Sie es mit Sicherheit? Wer greift ohne Ihr Wissen auf Ihre Daten zu? Wer hat durch die von Ihnen eingerichtete Perimetersicherheit hindurch Zugriff auf Ihre Endpoints? Blockiert Ihre derzeitige Antiviren-Software Malware tatsächlich und schützt sie Ihre Endpoints wirklich? In der feindseligen digitalen Welt der Gegenwart sind dies wichtige Fragen, die einer echten Antwort bedürfen.

Es ist an der Zeit, den Kampf gegen Cyberkriminalität aufzunehmen – und dieser Kampf beginnt beim Endpunkt. Im Whitepaper „Populäre Security-Irrtümer“ betrachten wir zehn Fallen, durch die IT-Abteilungen Cyberkriminellen den Zugriff auf den Endpunkt und damit den Diebstahl von Daten und Anmeldeinformationen ermöglichen. Es bedarf einer grundlegenden Veränderung der Einstellung von IT-Abteilungen, um Cyberkriminalität zu verhindern und Endpoints wie Anwender zu schützen.

Kaspersky Labs GmbH
Despag-Straße 3
85055 Ingolstadt
Deutschland

www.kaspersky.de
E-Mail: salesdach@kaspersky.de
Telefon +49 (0) 841 98 189 0
Telefax +49 (0) 841 98 189 100