Die Gefahren ändern sich – die Bedrohung bleibt

Winfried Naumann | Computer- und Medienservice, Systemsoftware und Kommunikation | w.naumann@cms.hu-berlin.de

Die meisten Angriffe richten sich immer noch gegen PCs mit Windows-Betriebssystemen. In diesem Beitrag wird gezeigt, wie sich die Gefährdungen verändert haben und wie die Benutzer sich auf diese Veränderungen einstellen müssen. Sicherheitsupdates für das Betriebssystem allein sind längst nicht mehr ausreichend – auch die Anwendungen müssen ständig aktualisiert werden, aktuelle Virenscanner versagen bei der Erkennung vieler Schädlinge und die Gefahren gehen eher von Webseiten als von Mail-Anhängen aus. Es wird immer wichtiger, dass die PCs durch ein Bündel von Sicherheitsmaßnahmen geschützt werden – einzelne Absicherungen sind den vielfältigen Gefahren nicht mehr gewachsen. Der überwiegende Teil des Artikels ist nicht betriebssystemspezifisch ausgerichtet, einige praktische Empfehlungen richten sich jedoch an Windows-Benutzer.

Durch neue Angebote und Dienste, neue Technologien und veränderte Anforderungen hat sich die Nutzung der Computernetze, vor allem die Nutzung des Internets, drastisch verändert, außerdem nimmt sie weiterhin stark zu. An diese Veränderungen haben auch die Angreifer ihre Methoden angepasst. Mit dem Missbrauch der Netze, z. B. für das Versenden von Spam-Mails, das Ausspähen vertraulicher Daten oder Angriffe auf wichtige Server, kann inzwischen sehr viel Geld verdient werden. Auch die Angreifer haben moderne Technologien zur Verfolgung ihrer Ziele zur Verfügung.

Welche Ziele verfolgen die Angreifer?

- Die kurzfristige Übernahme der Kontrolle über sehr viele PCs zum Aufbau von großen Bot-Netzen: Für das millionenfache Versenden von Spam-Mails oder den Angriff auf die Server eines bestimmten Unternehmens (z. B. eines Konkurrenten) können zahlungskräftige Kunden ein Bot-Netz mieten. Die Auftragnehmer steuern dann tausende von vorher infizierten Rechnern (Zombies), um damit genau die bezahlten Aufträge auszuführen.
- Phishing und Spionage: Durch die Installation von Schadsoftware, das Fälschen von Web-Seiten, (z. B. von Banken) oder die „Umlenkung“ der Benutzer auf entsprechend präparierte Web-Seiten versuchen die Angreifer, Anmelde-Daten (Accounts, Passwörter etc.) abzugreifen, um anschließend mit den Rechten dieser Benutzer weitere kriminelle Operationen ausführen zu können (z. B. vertrauliche Daten zu kopieren oder zu zerstören, Bankkonten zu leeren).
- Missbrauch (vor allem) von Servern, um sie als illegale Download-Server für Raubkopien von Software, Videos, Musik oder Kinderpornographie zur Verfügung stellen zu können

Sieht man sich diese Ziele an, kann kaum jemand behaupten, sein Rechner wäre für Angreifer uninteressant und braucht deshalb nicht vernünftig geschützt zu werden. Drei Beispiele:

- Für die Vorbereitung von Konferenzen müssen viele persönliche Daten von Konferenz-Teilnehmern (inkl. Kreditkarten-/Konto-Informationen) gesammelt werden.
- Auf Rechnern von Forschungsgruppen liegen (noch) nicht anonymisierte Daten aus psychologischen oder sportmedizinischen Tests, aus psychologischen oder soziologischen Fragebögen, Interviews oder auch vertrauliche Forschungsergebnisse, die in Kooperation mit Unternehmen entstanden sind.
- Mitarbeiter/-innen in Sekretariaten managen einen großen Teil des beruflichen und sogar persönlichen Lebens von leitenden Mitarbeitern und Professoren und verwalten Prüfungs- und andere Daten der Studierenden.

Und: Falls die auf der Festplatte gespeicherten Daten wirklich nicht interessant sind, dann taugt fast jeder PC noch als ferngesteuerter Zombie in einem Bot-Netz.

Welche Methoden werden benutzt, um PCs zu kompromittieren?

- In fast jedem Betriebssystem und fast jeder Anwendungssoftware gibt es Fehler (Sicherheitslücken). Werden diese Lücken vom Hersteller nicht durch Updates geschlossen oder die Updates vom Benutzer nicht installiert, können sie von Angreifern als Einfallstore genutzt werden, um Schadsoftware zu installieren oder das System für die Angreifer noch weiter zu öffnen.
- Benutzer gelangen mit ihrem Web-Browser auf Webseiten, die gezielt Sicherheitslücken im Browser oder in einem Media Player (z. B. beim Abspielen von Filmen) ausnutzen, um Schadsoftware auf den Rechner zu laden und dann auszuführen. Über Schadsoftware (Würmer), die bereits auf anderen Rechnern im lokalen Netz etabliert wurde, sind dann auch Angriffe auf weitere Rechner über nicht geschlossene Sicherheitslücken in diesen Systemen möglich.
- Viele Benutzer arbeiten unter Benutzerkennzeichen mit Administratorrechten (also viel mehr Rechten, als sie für ihre Arbeit eigentlich brauchen) und machen es Angreifern damit besonders leicht, Schädlinge im System zu installieren.

„Ich habe ein Antivirus-Programm installiert. Ist das nicht genug?“

Die im letzten Artikel [1] zum Thema Sicherheit von Windows-Clients vor etwa 4 Jahren aufgestellten Regeln zur sicheren Nutzung von PCs gelten immer noch, aber die Empfehlungen sind jetzt anders zu gewichten.

Virenscanner

Die Installation eines leistungsfähigen Virenscanners auf jedem Rechner (im HU-Netz McAfee VirusScan Enterprise) und das regelmäßige, möglichst automatische Aktualisieren der Virensignaturen (.dat-Dateien) gehört zu den Selbstverständlichkeiten. Unabhängige Tests verschiedener Antivirus-Produkte wie z. B in [2] zeigen, dass die meisten Virenscanner – verglichen mit Testergebnissen in den Vorjahren – ihre Aufgaben (Schutz des Rechners vor Schädlingen, Entfernung von Schädlingen) schlechter erfüllen und auch den gestiegenen Anforderungen, die sich aus den aktuellen Gefahren im Netz ergeben, noch nicht gewachsen sind. Warum ist das so?

- Die meisten Produkte stützen sich immer noch auf die signaturbasierte Erkennung von Viren. Zwangsläufig werden irgendwann alle Produkte daran scheitern: Die Zahl der verbreiteten Schädlinge wächst immer stärker. Obwohl einige Hersteller von Antivirus-Produkten schon mehrmals am Tag neue Updates bereitstellen, ist es für sie kaum noch möglich, die richtige Virensignatur rechtzeitig vor einem großen Angriff zu erstellen, zu testen und an die Kunden auszuliefern. Bot-Netze mit 100.000 ferngesteuerten Zombies können einen neuen Schädling in viel kürzerer Zeit an Millionen potentieller Opfer verbreiten. Die häufigen Signatur-Updates führen pro PC zu einem Download-Umfang zwischen 50 und 270 KByte pro Woche. Bereits die geringfügige Variation eines Virus (die auch von Laien durchführbar ist) ergibt eine andere Signatur, was dazu führt, dass er vom Scanner nicht mehr erkannt wird. Das Testen aller Dateien gegen eine so große Zahl von Virensignaturen führt zu enormen Leistungseinbußen auf den Rechnern und führt dazu, dass der Virenscanner auf älteren PCs inzwischen wieder zum Bremsklotz und von manchem Benutzer deshalb deaktiviert wird.
- Die signaturbasierte Erkennung von Viren muss also durch weitere Erkennungsmethoden ergänzt werden. Andere Methoden – die heuristische oder die verhaltensbasierte Erkennung von Schädlingen – sind bisher nur in wenigen Produkten und häufig noch sehr ungenügend implementiert. Dazu kommen oft schlechte Benutzeroberflächen (wie bei Personal Firewalls ist bei dieser Methode die Interaktion mit dem Benutzer wichtig!).
- Viele Antivirus-Produkte sind wegen eigener Sicherheitslücken in letzter Zeit oft selbst ein Sicherheitsproblem. Das ist besonders problematisch, weil sich diese Programme tief im Betriebssystem verankern müssen, um ihre Aufgaben erfüllen zu können.
- Antivirus-Produkte sollten inzwischen auch Root-Kits und Spyware aufspüren und unschädlich machen können, damit die Benutzer für diese Aufgaben nicht noch weitere Programme installieren (und zusätzlich pflegen!) müssen. Auch in diesen Punkten sind viele Produkte noch ungenügend.

Für eine große Einrichtung wie die Humboldt-Universität ergibt sich ein weiteres Problem: Wegen der großen Zahl der Virenscanner-Installationen im HU-Netz ist es schwer möglich, mal schnell den Anbieter zu wechseln, nur weil dessen aktuelle Sicherheits-Suite bestimmte Anforderungen besser erfüllt als das an der HU installierte Produkt (eine Frage des Preises ist es auch).

Um es deutlich zu sagen: Die vorangegangenen Ausführungen über die Virenscanner sollten nicht dazu führen, die Virenscanner zu deaktivieren oder sogar vollkommen wegzulassen! Schlussfolgerung: Virenscanner können nur eine (wichtige) Komponente im Schutzschild zur Absicherung des Computers sein – sie allein können Ihren Rechner nicht (zurzeit sogar immer weniger) schützen.

Personal Firewalls

Benutzer und Administratoren fragen uns häufig, ob sie zum Schutz ihres Rechners zusätzlich eine Firewall installieren sollen, um den ein- und ausgehenden Datenverkehr auf dem PC besser kontrollieren zu können. Windows XP Professional und Windows Vista (ab Business Edition aufwärts) enthalten eine einfache Firewall (die von Windows XP kann nur den eingehenden Verkehr kontrollieren). Mit den komplexen Einstellungen, die für eine wirksame Kontrolle des Datenverkehrs vom und zum PC nötig wären, sind die meisten Benutzer überfordert. Die Bedienung ist häufig zu kompliziert. Die Firewall wird zu weit geöffnet oder ganz abgeschaltet, wenn die Benutzer sich durch die Nachfragen der Software genervt und in ihrer Arbeit behindert fühlen. Das Ergebnis ist, dass der Datenverkehr kaum

noch begrenzt ist, die Benutzer sich aber in trügerischer Sicherheit wiegen, da sie ja zusätzlich eine Firewall installiert haben. Fast alle kostenlosen Personal Firewalls für Windows sind nur für den privaten Einsatz kostenlos – für den Arbeitsplatzrechner müsste eine Lizenz gekauft werden.

Die Empfehlung lautet: Benutzen Sie die eingebaute Firewall des Windows-Betriebssystems in der Standard-Einstellung oder noch besser in der Einstellung „ohne Ausnahmen".

Die (Un)Sicherheit der Anwendungssoftware

Kaum eine Webseite kommt inzwischen ohne aktive Inhalte (also: Skripte zur Navigation oder Multimedia-Inhalte wie z. B. Flash-Dateien) aus. Das führt dazu, dass man auf diesen Webseiten kaum noch navigieren kann oder viele Inhalte gar nicht angezeigt bekommt, wenn die Skripting-Fähigkeiten des Web-Browsers (Javascript, VBScript) deaktiviert sind oder das passende Plug-in/der Player für das angebotene Multimedia-Format nicht installiert sind. Der Trend geht schon seit langem dahin, dass im Browser (fast) alles darstellbar/abspielbar sein muss. Der Einsatz neuer Technologien wie z. B. Ajax macht es möglich, dass sogar ty-pische Office-Anwendungen vom Desktop teilweise ins Web „umziehen". Wachsende Anforderungen an mobiles Arbeiten und an die universelle Verfügbarkeit von Programmen und Daten führen dazu, dass sich der Arbeitsplatz vieler Benutzer immer stärker ins Web verlagert und dadurch die Anwendungen, mit denen sie mit dem Web „in Kontakt treten" – die Web-Browser, das Mail-Programm – eine größere Bedeutung erlangen. Ebenso wichtig sind die Betrachter (Viewer) und Player für die verschiedenen Medien-Formate (als Plug-in oder Add-on/Extension im Browser und im Mail-Programm oder als selbständige Programme, die bei Bedarf vom Browser oder vom Mail-Client zur Anzeige von Anhängen aufgerufen werden). Die meisten Benutzer haben Adobe Reader, Adobe Flash Player, Quick Time Player und einen weiteren Media Player auf ihrem Rechner installiert.

Auch die Angreifer haben sich darauf eingestellt. Der Anteil an Schadsoftware, die per Mail verteilt wird (und immerhin in der Regel als bewusste Aktion des Benutzers den Download oder das Öffnen von Dateien erfordert), ist stark zurückgegangen. Viel häufiger erfolgen die Angriffe inzwischen über entsprechend präparierte Webseiten, die dann Schwachstellen im Web-Browser, in Plug-ins oder im Media Player ausnutzen, um Hintertüren (Backdoors) im System zu öffnen und darüber weitere Schadsoftware nachzuladen und den Angriff fortzusetzen.

Sicherheitsanalysten stufen die Web-Browser inzwischen als Sicherheitsrisiko Nr. 1 ein [3]. Durch sichere Konfiguration des Browsers oder zusätzliche Add-ons (z. B. NoScript, Flashblock für den Browser Firefox) kann man die Risiken jedoch drastisch senken.

Zur Verdeutlichung der Probleme habe ich hier nur wenige Nachrichten einer einzigen Aprilwoche von *heise Security* [4] herausgepickt:

- 17.04. Firefox- und Safari-Updates schließen Sicherheitslücken
- 17.04. DivX-Player kommt beim Verarbeiten von Untertiteln aus dem Tritt (Angriff über manipulierte Untertitel W.N.)
- 17.04. Details zu Sicherheitsfixes in OpenOffice 2.4
- 18.04. Rechteausweitung durch Fehler im Windows-Kernel
- 18.04. ActiveX-Modul von Microsoft Works reißt Sicherheitslücke auf
- 21.04. Paypal will alte Browser blockieren (Update)
- 22.04. Photoshop führt eingeschleusten Code aus
- 22.04. Microsoft-Studie: Trojaner-Verbreitung hat stark zugenommen
- 22.04. Sophos-Studie: Zahl infizierter Webseiten hat rapide zugenommen
- 23.04. Schleswig-Holstein: 39 Prozent der Betriebe von Computerkriminalität betroffen
- 24.04. Hunderttausende Webseiten mit schädlichem JavaScript infiziert

Am Beispiel einer einzigen Anwendung soll das weiter illustriert werden: Der Media Player QuickTime für Windows der Fa. Apple (meistens im Paket mit iTunes) gehörte in den letzten Monaten in Bezug auf Sicherheitslücken zu den Spitzenreitern. Immer wieder war es möglich, dass Angreifer Rechner über kritische Lücken im Player infizieren konnten, siehe z. B. [5]. Innerhalb von 6 Monaten musste Apple 5 neue Versionen (7.3, 7.3.1, 7.4, 7.4.1, 7.4.5) der Software liefern, um Sicherheitslücken zu schließen. In der aktuellen Version 7.4.5 sind seit Wochen bekannte Sicherheitslücken nicht geschlossen. Dasselbe gilt für viele andere Anwendungen (Browser, Player, ...). Sie enthalten Lücken, die oft seit Monaten bekannt sind, vom Hersteller bisher aber nicht durch Updates beseitigt wurden. Man sollte sich nicht in einem falschen Sicherheitsgefühl wiegen: die Tatsache, dass keine Updates angeboten werden, bedeutet längst nicht, dass die Anwendung sicher ist.

Sicherheits-Updates für die Anwendungen

Windows-Anwender sind bei der Suche nach Updates weitestgehend auf sich allein gestellt, müssen sich also um die Updates für jedes Programm/Plug-in selbst kümmern. Linux-Benutzer (v. a. die, die eine der großen Distributionen wie OpenSUSE, Ubuntu, Debian oder Fedora einsetzen) können regelmäßig Updates für alle installierten Software-Pakete automatisch geliefert bekommen. Immerhin bietet Microsoft inzwischen als Alternative zum vorkonfigurierten Windows Update (liefert nur Updates für das Betriebssystem, Hardware-Treiber, den Internet Explorer und einige systemnahe Zusatzkomponenten) das erweiterte Microsoft Update an, das auch Office-Programme und zunehmend weitere (Microsoft-) Programme aktualisiert. Man muss den eigenen PC dafür konfigurieren, kann dann aber alle diese Updates automatisch beziehen. Updates für Software anderer Hersteller muss man weiterhin selbst suchen. Inzwischen bieten viele Programme die Möglichkeit, automatisch beim Start oder vom Benutzer initiiert nach verfügbaren Updates beim Hersteller zu suchen (z. B. die Browser Firefox und Opera, die Add-ons von Firefox, der Adobe Reader, das Java Runtime Paket usw.).

Dort, wo Programme es anbieten, das Suchen nach Updates und das Her-

unterladen automatisch durchzuführen und Sie über die Verfügbarkeit von Updates zu benachrichtigen, sollten Sie die Möglichkeit nutzen. Es ist zeitaufwendig, die Sicherheitsprobleme und Updates aller benutzten Programme zu verfolgen. Meistens wird die Aktualisierung der Programme dann aus Zeitgründen „vergessen". Das regelmäßige Verfolgen der Meldungen auf heise Security ist eine gute Möglichkeit, um sich in kompakter Form und möglichst zeitsparend über Sicherheits-Updates zu informieren.

In Kürze wird der CMS den Administratoren der Institute eine weitere Möglichkeit zur Verfügung stellen, sich über sicherheitsrelevante Software-Updates zu informieren (siehe Artikel „Überwachung von Software-Versionen" in diesem Heft).

Schlussfolgerung: Die regelmäßige Überwachung und Aktualisierung der Anwendungen ist mindestens genauso wichtig wie die des Betriebssystems. Auch diese Maßnahme ist noch nicht ausreichend.

Die wichtigsten Regeln: Wie bleibt der PC sicher?

Da die Beschreibung aller wichtigen Sicherheitseinstellungen hier nicht möglich ist, folgen zum Abschluss dieses Beitrages noch einmal unsere wichtigsten Empfehlungen, wie Sie Ihren PC sicher schützen können – wenigstens als Liste von Stichpunkten (die Aufzählung ist eine Rangfolge!):

- Sicherheits-Updates für das Betriebssystem regelmäßig installieren (per *Automatische Updates;* von jedem 2. Dienstag im Monat an sind neue Updates verfügbar; möglichst *Microsoft Update* nutzen);
- das Betriebssystem sicher konfigurieren (sichere Passwörter, keine ungeschützten Freigaben, sichere Zugriffsrechte im Dateisystem);
- die eingebaute Firewall des Betriebssystems benutzen – in der Standard-Einstellung oder noch besser: „ohne Ausnahmen";
- einen Virenscanner installieren und die Signatur-Updates regelmäßig automatisch installieren lassen (Download-Angebot des CMS: für das HU-Netz vorkonfiguriertes Paket McAfee VirusScan Enterprise, auf allen Rechnern einsetzbar); den *Scan bei Zugriff* immer aktiviert lassen; mindestens einmal wöchentlich einen Komplett-Scan der Festplatte durchführen;
- sichere Konfiguration und regelmäßiges Update der Anwendungen; Schwerpunkt: Anwendungen, mit denen man direkt mit dem Internet kommuniziert (Browser inkl. Add-ons und Plug-ins, Mail-Client, Betrachter, Media Player) oder Dateien aus dem Netz öffnet (zusätzlich die Office-Programme);
- die eingebauten Möglichkeiten vieler Anwendungen nutzen, nach Updates zu suchen/den Benutzer über Updates zu informieren; für Anwendungen, denen solche Funktionen fehlen: erledigen Sie die Update-Suche am besten am gleichen Tag wie die monatlichen Betriebssystem-Updates;
- verantwortungsbewusstes Verhalten des Benutzers (z. B. nicht ständig mit Administrator-Rechten arbeiten, Passwörter nicht weitergeben, zweifelhafte E-Mails, Websites und Downloads meiden bzw. vorher gründlich prüfen);
- auf dem Rechner möglichst zusätzlich ein Antispyware-Tool (Empfehlung: Spybot Search & Destroy, kostenlos) und ein Anti-Rootkit-Tool installieren und regelmäßig die Festplatte scannen;

Wie wirken die Sicherheitsmaßnahmen zusammen?

Sie verfolgen z. B. im Web einen interessanten Link und geraten dadurch auf eine Webseite, die so präpariert ist, dass bereits beim bloßen Laden der Seite über eine Sicherheitslücke im Web-Browser ein Programm (Downloader) auf Ihrem PC gespeichert wird, das dann weitere Schadsoftware laden kann.
Wie könnte das z. B. verhindert werden?

1. Bevor Sie auf den Link klicken, sehen Sie sich die angezeigte Adresse (URL) an, wenn der Mauszeiger über dem Link steht. Sie bemerken dabei, dass der Link Sie auf eine andere Web-Adresse mit zweifelhaftem Namen führt und klicken deshalb doch nicht auf den Link.
2. Sie haben den Link nicht kontrolliert, aber Ihr Browser ist auf dem aktuellen Stand. Die von der Webseite ausgenutzte Sicherheitslücke ist in der letzten Version des Browsers geschlossen worden. Der im Beispiel beschriebene Angriff kann deshalb auf Ihrem Rechner nicht funktionieren.
3. Die Schadsoftware wurde von der Web-Seite heruntergeladen, weil Ihr Browser nicht auf dem aktuellen Stand war. Der Virenscanner (die Komponente „Scan bei Zugriff") erkennt den Downloader jedoch schon beim Speichern auf der Festplatte, löscht ihn und warnt Sie.
4. Die Schadsoftware ist von der Web-Seite auf Ihren PC gelangt und leider auch vom Virenscanner nicht erkannt worden (die Virensignaturen waren nicht auf dem aktuellen Stand). Damit die Schadsoftware sich wirksam auf Ihrem PC einnisten kann, muss sie mit Administrator-Rechten ausgeführt werden. Da Sie in diesem Falle nur als normaler Benutzer angemeldet waren, ist (außer dem Download) bisher nichts weiter passiert. Inzwischen hat der Virenscanner neue Signatur-Updates heruntergeladen und der vorkonfigurierte wöchentliche Scan über die gesamte Festplatte hat deshalb den Schädling erkannt und entfernt.

Diese Beispiele sollten illustrieren, dass durch die mehrfache Absicherung sogar beim Versagen von 3 Sicherheits-Maßnahmen wie im Fall 4. (Benutzer unaufmerksam, Browser nicht aktuell, Virenscanner nicht aktuell) eine Kompromittierung des PCs unter Umständen noch verhindert werden könnte.

Zusammenfassung

Die Welt des Internets ist ein Abbild der realen Welt: sie ist nicht sicherer geworden. Um den eigenen Rechner vor Angriffen und Schädlingen zu schützen, muss man mehr Aufwand betreiben. Die Verantwortung bleibt bei den Benutzern der Rechner – der CMS und die Administratoren in den Einrichtungen können nur Wissen, Empfehlungen und Anleitungen beisteuern. Die Computerbetriebsordnung, die jeder Benutzer akzeptieren

muss, der sich im HU-Netz bewegt und gesetzliche Regelungen wie die Novelle des Strafgesetzbuches (StGB) zur Bekämpfung der Computerkriminalität (Einführung des neuen § 202c StGB – „Hackerparagraph“) nehmen jeden in die Pflicht, den eigenen Rechner vor Angriffen von außen zu schützen und sich verantwortungsbewusst zu verhalten.

Der Aufwand lohnt sich jedoch: es kostet noch viel mehr Zeit, einen kompromittierten Rechner komplett neu aufzusetzen oder mühselig verlorenen Daten hinterherzujagen. Noch immer ist für die Absicherung von PCs kein riesiger Aufwand nötig. Viele Aufgaben lassen sich durch Automatisierung erleichtern. Auch die Einhaltung der wichtigsten Regeln ist nicht so schwer.

Literatur

[1] Naumann, W.: *Sicherheit für Windows-Clients*. CMS-Journal 25/2004, S. 53-54

[2] Knop, D., Schmidt, J.: *Auf der Pirsch*. c't 01/2008, S. 92-100

[3] *heise Security: SANS-Hitliste der Sicherheitsrisiken: Browser und Webanwendungen führen*. http://www.heise.de/security/SANS-Hitliste-der-Sicherheitsrisiken-Browser-und-Webanwendungen-fuehren--/news/meldung/99671

[4] *heise Security*. http://www.heise.de/security/news

[5] *heise Security: Webseiten infizieren PCs über Lücke in Apples QuickTime*. http://www.heise.de/security/Webseiten-infizieren-PCs-ueber-Luecke-in-Apples-QuickTime--/news/meldung/99908

IRONPORT®

IronPort Systems ist eine Geschäftseinheit von Cisco und ein führender Anbieter von Anti-Spam-, Anti-Viren- und Anti-Spywarelösungen. Die Appliances von IronPort wurden für kleine Firmen bis hin zu Global 2000 Unternehmen entwickelt und spielen in der Netzinfrastruktur eines Unternehmens eine geschäftsentscheidende Rolle. Die innovativen Systeme sind einfach zu bedienen und bieten höchste Leistungsfähigkeit. Sie verwenden SenderBase®, die weltweit größte Datenbank zur Beobachtung und Bewertung von E-Mail und Web-Bedrohungen.

Unser Leistungsportfolio umfasst:
- E-Mail & Web Security Appliances
- E-Mail & Web Reputationsfilter
- E-Mail Verschlüsselung
- Erstklassige Contentfilter
- Präventive Schutzmechanismen

www.ironport.de

IronPort is now part of Cisco. CISCO