



Präventive Sicherheit: Die Spielregeln ändern

Bleiben Sie Gefahren für Ihr Netzwerk immer einen Schritt voraus





Einleitung: Die neuen Regeln

Am 13. August 2005 begann sich ein böartiger Computerwurm namens Zotob Bot im Internet zu verbreiten. Innerhalb von nur wenigen Tagen folgte mindestens ein Dutzend weiterer Würmer, die alle dieselbe „Plug and Play“-Schwachstelle in Microsoft®-Betriebssystemen ausnutzten. Bei einigen handelte es sich um Varianten von Zotob, andere waren völlig anders. Zu den betroffenen Organisationen gehörten große Nachrichten- und Medienunternehmen wie CNN, ABC, NBC, Associated Press und die New York Times.

Es gab jedoch ein Sicherheitsunternehmen, das seinen Kunden präventiven Schutz bot.

Dieser Vorfall verdeutlicht nicht nur die Herausforderung, vor der Unternehmen mit Internetpräsenz heute stehen, sondern zeigt auch die Lösung auf. Im Fall von Zotob hatte Internet Security Systems (ISS), heute ein IBM Unternehmensbereich, genau wie bei früheren Angriffen durch Sasser, Blaster und Slammer rechtzeitig vor dem Angriff entsprechende Abwehrmaßnahmen entwickelt. So konnten die Kunden von ISS (heute IBM Internet Security Systems) mögliche Schäden an ihrem Netzwerk und Unterbrechungen ihrer Geschäftsabläufe – nicht nur aufgrund des ersten Angriffs, sondern auch aller darauf folgenden Varianten – verhindern.

Dieses revolutionäre präventive Sicherheitskonzept hat IBM Internet Security Systems zu einem verlässlichen Sicherheitsanbieter gemacht, dem Regierungsbehörden und die weltweit größten Unternehmen vertrauen. Im Gegensatz zu traditionellen Sicherheitsmethoden, die Angriffe erst analysieren und entsprechend reagieren können, wenn diese bereits stattgefunden haben, wehrt eine Lösung für die präventive Sicherheit Gefahren aus dem Internet ab, bevor sie sich auf das Netzwerk auswirken können. Bis vor kurzem stellte IBM Internet Security Systems seinen Kunden diese präventive Sicherheit noch mit manuellen und daher komplexen Methoden bereit. Inzwischen wurden diese Methoden jedoch optimiert und automatisiert und in eine vereinfachte Plattform für die Internetsicherheit integriert, die Unternehmen jeder Größe ein Höchstmaß an Schutz bietet.

Mit dieser umfassenden Sicherheitsplattform legt IBM Internet Security Systems die Regeln für unterbrechungsfreie Geschäftsabläufe und die Einhaltung gesetzlicher Bestimmungen neu fest. Diese neuen Regeln setzen die Messlatte höher, an der sich Sicherheitslösungen messen lassen müssen.

- **Prävention statt Reaktion.** Angesichts der ausgeklügelten neuen Bedrohungen aus dem Internet können heutzutage nur wenige Sekunden über geschäftliche Verluste entscheiden. Vor diesem Hintergrund ist Prävention von entscheidender Bedeutung. Denn wer nur auf eine Bedrohung reagiert, kann sie nicht schnell genug abwehren.
- **Bei der Internetsicherheit geht es nicht so sehr um Netzwerke oder Hardware, sondern um die Software, die diese Systeme steuert** – genauer gesagt, um die Schwachstellen in dieser Software. Wenn Prävention der Schlüssel zur Sicherheit ist, dann ist die Fähigkeit, Schwachstellen in der Software zu finden und abzusichern, bevor sie ausgenutzt werden können, der Schlüssel zur Prävention. Auf Angriffen basierende Sicherheitsmethoden (z. B. das traditionelle Virenschutzmodell, das Angriffe analysiert, nachdem sie bereits gestartet wurden, und entsprechende Gegenmaßnahmen einleitet) spielen zwar nach wie vor eine Rolle. Heute setzt jedoch die schwachstellenbasierte Sicherheit neue Maßstäbe für Leistung und Prävention.
- **Echte Sicherheit ist dynamisch – sie ist kein Massenprodukt und keine selbstverständliche Eigenschaft der Infrastruktur.** Da die Software immer komplexer wird, vervielfachen und verändern sich auch die Gefahren für die Software immer rascher. Seit 1990 hat die Zahl der Softwareanwendungen auf Netzwerkservern und -geräten exponentiell zugenommen, und diese Anwendungen bergen nach wie vor eine Vielzahl verschiedener Sicherheitsrisiken. Eine effektive Sicherheitslösung muss diesem Trend stets voraus bleiben. Um sicherzustellen, dass Unternehmen einen Vorsprung vor potenziellen Angreifern haben, wendet eine Lösung für die präventive Sicherheit Erkenntnisse und Techniken an, die aus innovativen und offensiven Forschungsmethoden abgeleitet wurden und ständig weiterentwickelt werden.
- **Die präventive Sicherheit kommt möglichen Gefahren zuvor:** Sie sorgt dafür, dass ein Unternehmen Gefahren für die Sicherheit seines Netzwerks stets einen Schritt voraus bleibt.
- **Prävention verringert den Aufwand für die Sicherheit und trägt so zu Kostensenkungen bei.** Unternehmen kaufen Technologie, um ihre IT-Umgebung zu vereinfachen, aber traditionelle Sicherheitslösungen (Einspielen von Patches, Intrusion-Detection-Systeme, Firewalls etc.) können den Aufwand sogar noch erhöhen. In manchen Fällen sind sie für die Hälfte der steigenden Kosten im Bereich der Sicherheit verantwortlich. Eine wirksame Kostendämmung erfordert bessere Sicherheit. Indem Gefahren abgewehrt werden, noch bevor sie sich auf ein Unternehmen auswirken können, trägt die präventive Sicherheit zur Verringerung der Arbeitsbelastung und Kosten bei.
- **Eine bessere Lösung:** Werden Technologien für präventive Sicherheit innerhalb einer integrierten Plattform bereitgestellt, profitieren Unternehmen von umfassendem, wirksamem Schutz, der skalierbar ist und zentral gesteuert werden kann.



Unternehmen brauchen ein strategisches Konzept für die Internetsicherheit

Das Internet ist heute Motor geschäftlicher Transaktionen. Das bedeutet, dass die Internetsicherheit der Schlüssel zu geschäftlichem Erfolg ist. Die Internetsicherheit entscheidet maßgeblich darüber, wie gut ein Unternehmen interne Netzwerke managen, neue Technologien und Anwendungen integrieren und neue gesetzliche Bestimmungen und Branchenstandards einhalten kann – während Sicherheitsbedrohungen immer vielfältiger und ausgefeilter werden. Angesichts des Ausmaßes der Bedrohung ist die einfache Erweiterung des unzulänglichen Flickwerks aus taktischen und „reaktiven“ Einzellösungen für die Sicherheit keine wünschenswerte Option. Die Internetsicherheit sollte als strategische geschäftliche Notwendigkeit betrachtet werden. Das Ziel ist die Kombination effektiver präventiver Sicherheitstechnologien innerhalb einer integrierten Plattform, die das gesamte Unternehmen (Server, Netzwerke und Desktops) abdeckt. Diese Plattform lässt sich einfach ausbauen, liefert Erkenntnisse, die sich in konkrete Maßnahmen umsetzen lassen, und erlaubt ein vereinfachtes zentrales Management.

Lassen Sie überholte Vorstellungen und unangenehme Überraschungen hinter sich

Trotz all der Mühen und Kosten, die auf die Sicherheit verwendet werden, lässt sich die Unternehmensumgebung von heute durch konventionelle Sicherheitslösungen nicht ausreichend schützen. Häufig müssen Unternehmen erleben, wie ihre teuren und komplizierten Sicherheitssysteme durch einen einzelnen, unvorhergesehenen Angriff aus dem Internet überwunden werden. Folglich sind sie ständig gezwungen, auf Gefahren zu reagieren – d. h. im Fall von Sicherheitsverstößen fieberhaft zu versuchen, die Lage wieder unter Kontrolle zu bringen und die Ordnung wiederherzustellen. Die Internetsicherheit wirkt sich auf praktisch alle Aspekte der Unternehmensführung, der Migration von Technologien und des geschäftlichen Wachstums aus. Daher sollten die Führungskräfte in Unternehmen höhere Erwartungen an die Funktionalität von Lösungen für die Internetsicherheit stellen. Sie sollten Sicherheitslösungen verlangen, die sowohl effektiv als auch einfach zu managen sind, und sie sollten die Rolle der Sicherheit in einem weiter gefassten, strategischeren Kontext betrachten.

Höhere Produktivität durch bessere Netzwerksicherheit

Unternehmensnetzwerke wachsen schnell, da nicht nur entfernte Niederlassungen und Telearbeiter, sondern auch Lieferanten, Kunden, Auftragnehmer und weitere externe Organisationen und Einzelpersonen in das Netzwerk eingebunden werden. Zudem sind neue Technologien wie mobile Netze, Smartphones und VPN-Zugriff (Virtual Private Network) auf dem Vormarsch und werden immer häufiger implementiert. Dieser integrierte Ansatz bringt enorme geschäftliche Vorteile mit sich, z. B. kürzere Lieferketten, schnellere Reaktionszeiten gegenüber Kunden und geringere Fehlerraten sowie generelle Kostensenkungen. Leider sind konventionelle Sicherheitsmethoden von der stark wachsenden Anzahl an Netzwerkbenutzern oftmals überfordert, was dazu führen kann, dass sie externen Benutzern „Standardzugriff“ auf kritische Systeme und Daten gewähren. Eine effektive Strategie für die Internetsicherheit sollte unternehmensweiten Schutz gewährleisten und Unternehmen die Möglichkeit bieten, die Grenzen ihres Netzwerks ohne Risiko auszuweiten. Dadurch profitieren sie von weiteren Produktivitätssteigerungen, Kostensenkungen und besserer Wettbewerbsfähigkeit auf einem dynamischen globalen Markt.

Stellen Sie nicht nur die Netzwerkverfügbarkeit, sondern auch optimierte Bandbreite sicher

Unvorhergesehene Ausfallzeiten sind ein akuter Notfall für ein Unternehmen, vergleichbar einem Herzinfarkt beim Menschen. Das erklärt, warum Netzwerkmanager solche Ausfälle unbedingt vermeiden wollen. Andererseits scheint der Verlust von Bandbreite – der eher mit einer chronischen, schleichenden Krankheit zu vergleichen ist – trotz seiner schädlichen Auswirkungen auf die reibungslosen Geschäftsabläufe eines Unternehmens für gewöhnlich toleriert zu werden. Unbefugter Datenverkehr im Netzwerk beansprucht Bandbreite, die eigentlich zur Unterstützung geschäftskritischer Anwendungen benötigt wird. Er verringert die Netzwerkeffizienz, führt zu einem Anstieg der Kosten für die Unterstützung der Infrastruktur und öffnet einer Vielzahl von Sicherheitsbedrohungen Tür und Tor.

Ein strategisches Konzept für die Internetsicherheit kann sowohl Ausfälle als auch Bandbreitenverluste vermeiden helfen. Denn es kombiniert Funktionen für die Erkennung von Unregelmäßigkeiten und die Abwehr unbefugter Zugriffe mit weiteren Sicherheitstechnologien in einer integrierten Plattform, die das gesamte Netzwerk schützt – vom Kern bis zu den äußersten Grenzen.

Die Internetsicherheit muss als strategische geschäftliche Notwendigkeit betrachtet werden.

Nutzen Sie neue Anwendungen ohne neue Risiken

Unternehmen sind in regelmäßigen Abständen mit Sicherheitsproblemen bei bereits etablierten Technologien konfrontiert. Dieses Problem wird durch die rasche Einführung neuerer Anwendungen wie VoIP (Voice over Internet Protocol), CRM (Customer Relationship Management) und anderen noch deutlich verschärft. Viele dieser Technologien bringen durch eine Vielzahl neuer Einstiegspunkte und die direkte Interaktion mit kritischen Back-Office-Anwendungen neue Sicherheitsrisiken mit sich, die das Unternehmen gefährden. Wie bei jeder neuen Generation von Technologie stoßen konventionelle Sicherheitslösungen auch hier an ihre Grenzen. Denn konventionelle Sicherheitslösungen sind darauf ausgelegt, bekannte Gefahren zu bekämpfen. Doch Gefahren im Zusammenhang mit neuer Technologie sind größtenteils noch unbekannt. Aus diesem Grund muss sich eine strategische Lösung für die Internetsicherheit an Schwachstellen und nicht an Angriffen orientieren. Es ist schlicht unmöglich, die unendliche Anzahl möglicher Angriffe auf eine neue Technologie vorherzusehen. Mit einer offensiven Erforschung von Sicherheitslücken und der Entwicklung geeigneter Technologien ist es jedoch erwiesenermaßen möglich, sich auf die Schwachstellen zu konzentrieren, die bei solchen Angriffen ausgenutzt werden können. Außerdem kann auf diese Weise ein System aufgebaut werden, das Verhaltensmuster erkennt, die auf neue und zuvor noch nicht kategorisierte Angriffe hinweisen.

Präventive Sicherheit: Die Spielregeln ändern



Halten Sie mit dem Wachstum Ihres Netzwerks Schritt und optimieren Sie gleichzeitig das Sicherheitsmanagement

Wachsende Netzwerke enthalten für gewöhnlich hunderte oder gar tausende von Sicherheitsanwendungen und -geräten, die Schutz vor einer immer größeren Anzahl unterschiedlicher Bedrohungen bieten – und die meist weder miteinander kommunizieren noch aufeinander abgestimmt sind. Diese verschiedenen Ebenen unterschiedlicher und voneinander unabhängiger Systeme vergrößern die Netzwerkkomplexität und führen zu einem Anstieg der Administrationskosten und höherem Wartungsaufwand.

Zudem kann eine solche Ansammlung taktischer Fixes das Unternehmen in der Regel nicht ausreichend schützen, da diese Fixes grundlegende Schwachstellen auf Unternehmensebene nicht beseitigen. Tatsächlich können sie Angreifern sogar den Weg bahnen.

- *Funktionale „Grauzonen“ zwischen den einzelnen Produkten bleiben mögliche Eingangspunkte für Angreifer.*
- *Es gibt keine einheitliche Architektur oder technologische Grundlage, die die Implementierung der Anwendungen vereinfacht.*
- *Die verschiedenen Produkte lassen sich weder zentral darstellen oder managen, was eine effektive Kontrolle und Dokumentation der Funktionen ermöglichen würde, noch besteht die Möglichkeit, die erforderlichen präzisen Berichte zu erstellen.*

Auch diese Probleme lassen sich mit einer strategischen, plattformorientierten Herangehensweise an die Internetsicherheit lösen. Eine Plattform kann einer Technologie die nötige Skalierbarkeit verschaffen – für eine wachsende Anzahl an Benutzern und Standorten – und außerdem eine Verschlechterung der Leistung oder eine deutlich größere Komplexität beim Management vermeiden.

Effektive Sicherheit kann die Einhaltung von Bestimmungen vereinfachen

Die Einhaltung gesetzlicher Bestimmungen erschwert die Anstrengungen für effektive Internetsicherheit spürbar. Bestimmungen wie HIPAA, Sarbanes-Oxley, Basel II und Gramm-Leach-Bliley Act bergen verschiedene rechtliche und finanzielle Risiken. Darüber hinaus kann eine nachgewiesene Nichteinhaltung von Bestimmungen oder eine erforderliche Veröffentlichung von Sicherheitsverletzungen einem Unternehmen negative Publicity einbringen und dem Unternehmens- und Markenwert schaden. Für die Einhaltung solcher gesetzlicher Bestimmungen ist und bleibt der Kunde verantwortlich. Ein effektives Sicherheitssystem kann den Kunden jedoch dabei unterstützen, bestimmte gesetzliche Bestimmungen einzuhalten.

Aus strategischer Sicht sollte die Internetsicherheit Unternehmen aus zwei Gründen bei der Einhaltung gesetzlicher Bestimmungen unterstützen:

- *Effektive Sicherheit verringert das Risiko von Sicherheitsproblemen.*
- *Eine plattformorientierte Strategie für die Internetsicherheit sollte zu größerer Transparenz beitragen und so die Erstellung der notwendigen Berichte ermöglichen.*

Die Suche nach dem heiligen Gral der Sicherheit

Einige Unternehmen wiegen sich noch immer in dem Glauben, dass sie von konventionellen Sicherheitssystemen ausreichend geschützt sind. Andere vertreten die landläufige Meinung, dass die Risiken einfach unvermeidlich sind und reaktiver Schutz die einzige Alternative ist.

Die Vision einer Sicherheitslösung, die Gefahren abwehren kann, bevor sie das Unternehmen beeinträchtigen – eines Systems, das automatisch und kosteneffizient sowohl vor bekannten als auch unbekanntem Angriffen schützt – gab es schon immer. Sie scheint jedoch unerreichbar.

Tatsächlich kann diese Vision in die Realität umgesetzt werden. Hierzu ist lediglich eine integrierte, präventive Plattform erforderlich, die fest in der Erforschung von Schwachstellen begründet ist. Diese Methode ist die einzige geeignete Lösung, da sie drei wesentlichen Anforderungen gerecht wird:

- *Sie verhindert auf effektive Weise sicherheitsbedingte Verluste für das Unternehmen.*
- *Sie bietet die Möglichkeit, Sicherheit als langfristige Investition zu planen und zu managen, indem sie eine Grundlage für die Weiterentwicklung von Sicherheitstechnologien schafft.*
- *Sie sorgt für ein hohes Maß an Schutz durch Sicherheits-services, die bedarfsgerecht bereitgestellt werden.*

Denken Sie neu darüber nach, was Sicherheitstechnologie leisten sollte

Auf Funktionsebene ähnelt das Sicherheitsrisiko einem undichten Dach, das einem stärker werdenden Regenguss Stand halten muss. Die Frage ist: Was tun Sie, um die undichte Stelle zu flicken und Schäden durch den Regen zu vermeiden? Wählen Sie eine Lösung, die einzelne Regentropfen untersucht, während sie fallen? Oder eine Lösung, die die undichten Stellen in Ihrem Dach findet und beseitigt?

Auf strategischer Ebene besteht die Herausforderung darin, über das Flicken der Löcher im Dach – d. h. der Sicherheitslücken in Ihrem Unternehmen – hinauszugehen und den Wert der Sicherheitslösungen zu steigern. In diesem Zusammenhang stellt sich die Frage: Was kann die Sicherheitsforschung für Ihr Unternehmen leisten?

Um Sicherheitsbedrohungen wirklich zu verstehen, müssen Sie sich die Software in Ihrem Unternehmen ansehen, die allzu oft einem Schweizer Käse ähnelt

Unternehmen sind auf Software angewiesen, einschließlich Geschäftsanwendungen, Back-Office-Software und Netzwerkbetriebssystemen. Doch praktisch jede Software weist Sicherheitslücken – Fehler im Code – auf. Je komplexer die Software wird und je mehr neue Versionen und Updates hinzukommen, desto größer wird die Menge des Codes und die Anzahl der Fehler. Diese Sicherheitslücken sind, um auf unser Beispiel zurückzukommen, die undichten Stellen im Dach Ihres Unternehmens. Die wachsende Anzahl an Softwareschwachstellen führt zu einer ständigen Zunahme möglicher Bedrohungen, da theoretisch jede Schwachstelle durch mehrere Methoden ausgenutzt werden kann. Viele dieser Methoden sind ausgesprochen raffiniert und können erheblichen Schaden anrichten.

Präventive Sicherheit: Die Spielregeln ändern



Die Erforschung von Schwachstellen ist ein wesentlicher Bestandteil der präventiven Sicherheitsplattform, für die IBM Internet Security Systems Pionierarbeit geleistet hat. IBM Internet Security Systems deckt Schwachstellen auf, noch bevor Angriffe gestartet werden können, und bietet so sicheren Schutz vor den größten Gefahren aus dem Internet. Und mit der Virtual Patch-Technologie von IBM Internet Security Systems können Unternehmen auf das routinemäßige Einspielen von Notfallpatches verzichten. Denn mit dieser Technologie können sie Sicherheitslücken in der Software abschirmen, bis permanente Patches getestet und anschließend im Rahmen der üblichen, planmäßigen Wartung implementiert werden können. In unserem Beispiel des undichten Dachs ist die Virtual Patch-Technologie mit einer Schutzplane vergleichbar, die eine undichte Stelle abdeckt, bis das Dach schließlich repariert wird.

Eine auf Prävention basierende Sicherheitsplattform liefert wichtige Erkenntnisse für Unternehmen

Die Sicherheitsplattform von IBM Internet Security Systems sorgt für zentrale Transparenz und Kontrolle über die gesamte Sicherheitsinfrastruktur des Unternehmens. Dieser Ansatz ermöglicht es Führungskräften, die Sicherheit als strategische Ressource des Unternehmens zu nutzen. Das System wurde für die folgenden Ziele konzipiert:

- *Schwachstellen werden erkannt, zugeordnet und beseitigt.*
- *Sicherheitsressourcen werden zugeordnet und zentral verwaltet.*
- *Neue Benutzer werden erkannt und dokumentiert.*
- *Die Effizienz der Netzwerkbandbreite wird optimiert.*
- *Sicherheitsbedingungen und -ereignisse werden in Berichten dokumentiert.*
- *Patches werden im Rahmen der Routinewartung eingespielt.*
- *Sicherheitsinformationen werden effizient zwischen Abteilungen und Funktionen ausgetauscht.*
- *Die Anzahl der Anfragen beim Help-Desk wird reduziert.*
- *Neue Anwendungen werden vor der allgemeinen Implementierung effektiver getestet und bewertet.*
- *Neue Sicherheitsanwendungen werden auf einer gemeinsamen Plattform implementiert und betrieben.*
- *Prozesse für das Risikomanagement werden effektiver koordiniert.*
- *Die Verfügbarkeit und Zuverlässigkeit des Netzwerks können verbessert werden.*

Die Sicherheitsplattform von IBM Internet Security Systems

IBM Internet Security Systems kombiniert drei wichtige Elemente für die Bereitstellung umfassender präventiver Sicherheit:

- 1) erstklassige Forschung und Entwicklung,
- 2) weltweite Security Operations Center (SOCs) und
- 3) eine vereinheitlichte Sicherheitsplattform.

IBM Internet Security Systems nimmt eine führende Position im Bereich der Sicherheitsforschung und -innovation ein, unter anderem bei der Erfindung von Technologien für die Schwachstellenanalyse und für die Erkennung und Abwehr unbefugter Zugriffe. Wie kaum ein anderer Anbieter ist IBM Internet Security Systems in der Lage, die präventive Sicherheit bereitzustellen, die im Internet tätige Unternehmen heute brauchen. Aus der Kombination der Forschungs- und Entwicklungsorganisation IBM Internet Security Systems X-Force, der globalen Präsenz der IBM Internet Security Systems SOCs und Managed Services und der Sicherheitsplattform von IBM Internet Security Systems ergibt sich eine der fortschrittlichsten und umfassendsten Sicherheitslösungen, die heute verfügbar sind.

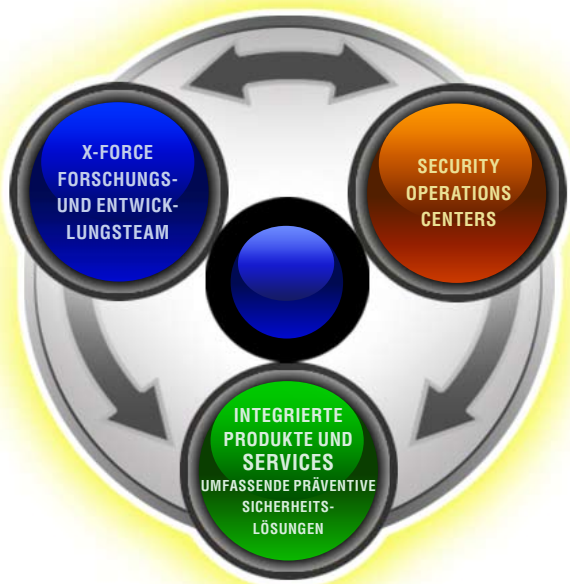
IBM Internet Security Systems X-Force – erstklassige Forschung und Entwicklung

Eine offensive, fundierte Sicherheitsforschung steht – und stand schon immer – bei IBM Internet Security Systems und allen Produkten und Services des Unternehmens im Mittelpunkt. Das Forschungs- und Entwicklungsteam IBM Internet Security Systems X-Force nutzt innovative Forschungsmethoden zur Analyse von Geschäftsanwendungen, Back-Office-Software und Netzwerkbetriebssystemen, die wesentliche Bestandteile der E-Commerce-Infrastruktur sind. Die herausragenden Erkenntnisse des X-Force-Teams in Bezug auf Softwareschwachstellen bilden die Grundlage für die präventiven Sicherheitslösungen von IBM Internet Security Systems.

IBM Internet Security Systems SOC – unser „Ohr am Puls der Zeit“

IBM Internet Security Systems kümmert sich rund um die Uhr, an sieben Tagen pro Woche, um den Betrieb der Sicherheitsinfrastruktur von vielen der sicherheitssensibelsten Unternehmen und Behörden weltweit. Durch die Überwachung hunderter global verteilter Netzwerke gelingt es IBM Internet Security Systems, ein Gefühl für die Aktivitäten im Internet zu gewinnen und so unbekanntes Exploits voraus zu bleiben. Die Sicherheitsspezialisten von IBM Internet Security Systems analysieren über mehrere SOC hinweg „Internet-Klatsch“ und verdächtigen Datenverkehr im Netz. Sie beobachten und untersuchen Angriffstechniken und lernen dabei, diese nachzustellen, vorauszuahnen und abzuwehren.

IBM INTERNET SECURITY SYSTEMS



Präventive Sicherheit: Die Spielregeln ändern



Die Sicherheitsplattform von IBM Internet Security Systems setzt neue Maßstäbe

Mit seiner Sicherheitsplattform hat IBM Internet Security Systems eine einfache, integrierte Lösung geschaffen, die allen sicherheitsbewussten Unternehmen präventiven Schutz bietet.

IBM Internet Security Systems hält ein Angebot an innovativen Sicherheitsanwendungen und -services bereit, die entweder als eigenständige Lösungen oder kombiniert in einem modularen, integrierten System erhältlich sind. Die Sicherheitsplattform von IBM Internet Security Systems vereint leistungsstarke Technologien in einer durchgängigen Komplettlösung. Sie beinhaltet nicht nur ausgereifte Technologien für die Abwehr unbefugter Zugriffe und die Erkennung von Unregelmäßigkeiten sowie für Firewall, VPN, Schwachstellensuche und Virenschutz, sondern auch Funktionen für die Mailsicherheit und Filter für Webinhalte. Zudem kann die Plattform mit Lösungen für Desktops, Server, Netzwerke und Gateways das gesamte Netzwerk abdecken. Alle Sicherheitsanwendungen der Sicherheitsplattform von IBM Internet Security Systems lassen sich von praktisch jedem beliebigen Standort aus steuern. Für die Sicherheitsplattform werden zwei verfügbare Bereitstellungsoptionen angeboten. Die Kunden können ihre Netzwerkinfrastruktur entweder in Eigenregie betreiben oder die Überwachung und den Betrieb der unternehmensweiten Netzwerkinfrastruktur IBM Internet Security Systems überlassen.

Die Komponenten der Sicherheitsplattform von IBM Internet Security Systems stellen eine revolutionäre Architektur dar, die Mehrwert durch umfassende Sicherheit schafft.

- *Einheitliche, integrierte Sicht des Netzwerks (Einhaltung von Bestimmungen, Reporting)*
- *Erweiterbare Plattform und Services*
- *Korrelationen und Integration mehrerer Datenquellen*
- *Zugrunde liegende herausragende Appliances*
- *Mögliche Integration innovativer Technologien (z. B. Anomaly Detection Service)*
- *Ausgelagertes Sicherheitsmanagement rund um die Uhr*
- *Höhere Systemverfügbarkeit und -leistung ohne enorme Investitionen in Technologie oder Ressourcen*
- *Sichere Managed Protection Services*

Fazit

Im Internet tätige Unternehmen müssen sich nicht länger auf reaktive Sicherheitsverfahren verlassen. Das Risiko enormer geschäftlicher Verluste durch ausgeklügelte neue Internetgefahren, neue gesetzliche Bestimmungen und die ständig steigenden Kosten für das Management veralteter Sicherheitsstrategien haben die Führungskräfte in Unternehmen aufgerüttelt. Die optimale Sicherheitsstrategie für die Lösung dieser Probleme heißt Prävention. Präventive Sicherheit erfordert erstklassige Forschungsarbeit, einen Blick für neue Trends und Techniken bei Sicherheitsbedrohungen und eine optimierte und kostengünstige Plattform für die Bereitstellung innovativer Sicherheitslösungen auf Wissensbasis. Präventive Sicherheit ist die einzige Lösung, mit der sicherheitsbewusste Unternehmen möglichen Gefahren immer einen Schritt voraus bleiben. IBM Internet Security Systems erfüllt die besten Voraussetzungen dafür, Ihnen diese Lösung bereitzustellen.

IBM Internet Security Systems verfügt über umfangreiches Know-how, innovative Forschungsmethoden und komplexe Technologien, die für präventive Sicherheit erforderlich sind. Die Angebote von IBM Internet Security Systems sind darauf ausgelegt, Ihnen diese Vorteile in benutzerfreundlichen Appliances, Softwareprodukten und Managed Services zur Verfügung zu stellen.

Warum IBM Internet Security Systems?

Tausende der weltweit führenden Unternehmen und Behörden vertrauen der Sicherheitsberatung und den präventiven Lösungen für die Sicherheit von Netzwerken, Desktops und Servern von IBM Internet Security Systems. IBM Internet Security Systems gilt als führend im Bereich der Sicherheit. Seine integrierte Sicherheitsplattform schützt automatisch vor bekannten und unbekanntem Gefahren, stellt die Verfügbarkeit des Netzwerks sicher und wehrt Onlineangriffe ab, bevor sie die Ressourcen eines Unternehmens beeinträchtigen können. Die Produkte und Services von IBM Internet Security Systems basieren auf der proaktiven Sicherheitsforschung des X-Force-Teams – einem Forschungs- und Entwicklungsteam, das weltweit als unbestrittene Autorität auf dem Gebiet der Erforschung von Sicherheitslücken und -bedrohungen angesehen wird. Die Produktreihe für präventive Sicherheit wird durch die umfangreichen IBM Managed Security Services ergänzt.

Wenn Sie mehr über IBM Internet Security Systems und präventive Sicherheit erfahren möchten, besuchen Sie uns unter:

ibm.com/services/de/iss



IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:

ibm.com

IBM, das IBM Logo und ibm.com sind eingetragene Marken der IBM Corporation.

Virtual Patch und X-Force sind Marken der IBM Corporation in den USA und/oder anderen Ländern.

Microsoft ist eine Marke der Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

© Copyright IBM Corporation 2007
Alle Rechte vorbehalten.