

bwmirror

Security-Magazin der **bw digitronik**

Nr. 2|2010

Wir sind umgezogen!



Log-Management-Lösung für KMUs.

Windows 7 und IT-Security.

EFG Bank setzt bei Endpoint Security auf Lumension Device Control.

Unsere neue Adresse: Uster West 30, 8610 Uster.

On the move 2010.

2010 ist ein bewegtes Jahr: von der Bankenkrise zur Eurokrise. Von Windows XP auf Windows 7. Von der Strickstrasse 15 nach Uster West 30. Und wird's jetzt besser?

Zuerst wollen wir Sie auf diesem Weg informieren, dass bw digitronik ag per Anfang August in eine neue Location umgezogen ist: Uster West 30 in Uster. Wir freuen uns, Sie in unseren neuen Räumlichkeiten willkommen zu heissen!

ArcSight hat speziell für kleinere und mittlere Unternehmen eine Log-Management-Lösung als Software-Version herausgebracht, welche für einen tieferen Preis den gleichen Funktionsumfang bietet. Die News dazu finden Sie auf dieser und auf der nächsten Seite.

Einige Unternehmen haben nach einer Phase des Abwartens dieses Jahr mit der Migration auf Windows 7 begonnen. Die Definition eines neuen Standard Clients muss auch eine Überprüfung der Sicher-



heitsarchitektur beinhalten. Hier bietet McAfee neue, interessante Lösungen für mehr Sicherheit und bessere Verwaltbarkeit an den Endpunkten. Lesen Sie mehr auf den Seiten 4–5.

Die grossen Zusammenhänge können wir für Sie leider nicht beeinflussen. Aber mit uns an Ihrer Seite, im Bereich Informationssicherheit, können wir die Eingangsfrage beantworten: Ja, es wird besser! Gerne beraten wir Sie persönlich und kompetent. Fordern Sie uns heraus!

Herzlichst

Paul Hasen
Vice President Sales

Log-Management-Lösung für KMUs

ArcSight 4.5 verfügbar, als Appliance oder als reine Software-Version!

ArcSight Logger bietet marktführendes, kosteneffizientes Management von jeglichen Logdaten für alle Kundenbedürfnisse. Neu ist ArcSight Logger auch als Software-Version verfügbar, was diese Lösung für kleinere und mittlere Unternehmen attraktiv macht.

Entwicklung der Anforderungen an das Log Management

Logs wurden ursprünglich gesammelt, um verschiedene Aufzeichnungen zu haben, welche dann im Rahmen von detaillierten forensischen Analysen nach Cyberattacken untersucht werden konnten. Auch wurden Logs gesammelt, um Nachweise für verschiedene Audits bereitzustellen, für die Unterstützung bei der Applikationsentwicklung und zum Verbessern des IT Service Levels. Früher waren Log-Analysen stark auf einzelne Bereiche beschränkt und wurden vor allem von der IT-Abteilung genutzt und verwaltet. Die meisten bisherigen Produkte wurden dafür entwickelt, um Logs von spezifischen Datenquellen zu sammeln und um einzelne Probleme zu lösen. Doch diese Tools sind nicht geeignet, um die gegenwärtigen Herausforderungen zu bewältigen, die sich heute IT-Teams stellen.

Unternehmen kämpfen aktuell mit sich rasch weiter entwickelnden Sicherheitsbedrohungen, mit wachsenden Compliance-Auflagen und stetig höheren IT-Service-Level-Anforderungen. Die

Fragen, welche durch die Analyse von Logdaten beantwortet werden müssen, sind bedeutend umfassender als in der Vergangenheit. Sie beziehen sich nicht mehr nur auf einzelne Systeme, sondern können die ganze Infrastruktur umfassen.

ArcSight Logger: Eine umfassende Log-Management-Lösung

Eine zeitgemässe, umfassende Log-Management-Lösung muss einem Unternehmen erlauben, alle möglichen Logs aus den unterschiedlichsten Quellen zu sammeln, Verschiedenes zu analysieren und eine maximale Performance zu einem guten Preis-Leistungs-Verhältnis bieten. Zudem sollte es möglich sein, die Interessen von verschiedenen Gruppen abzudecken, egal, ob es um Applikationsentwicklung oder um Compliance geht. ArcSight Logger vereint alle genannten Anforderungen in einer Lösung und bietet folgenden Leistungsumfang: Reporting, Alerting, Suche und Analyse aller möglichen Unternehmensinformationen. Die gesammelten Daten werden in einem standardisierten Format gespeichert, was eine komfortable und rasche Analyse ermöglicht. So können die grossen Mengen an Daten effizient verwaltet und ausgewertet werden. ArcSight Logger kann von unterschiedlichsten Teams spezifisch eingesetzt werden oder erweitert als unternehmensweite Log-Management-Lösung zum Einsatz kommen. Informationen können so einfach gemeinsam genutzt werden, was zu tieferen Gesamtkosten führt.

Sammelt sämtliche Logdaten

ArcSight Logger unterstützt die Sammlung von Rohdaten (sog. Raw-Format), von strukturierten sowie unstrukturierten Logs von sämtlichen Syslog und anderen file-basierten Log-Quellen. ArcSight kann mit seinen über 300 verfügbaren ArcSight Connectors standardmässig eine riesengrosse Anzahl Datenquellen anzapfen. Zusätzlich steht mit ArcSight FlexConnector ein Framework zur Verfügung, um kundenspezifische Quellen oder eigenentwickelte Applikationen ins Log Management einzubinden. ArcSight Connectors können entweder als separate Software oder als Appliances in Datacentern oder in Zweigniederlassungen zum Sammeln von Logdaten eingesetzt werden. ArcSight Connectors liefern auch Bandbreiten-Kontrollen, Log-Traffic-Priorisierungen, lokales Daten-Caching, End-to-End-Verschlüsselung und weitere Optionen, um Datenverluste und den Einfluss auf unternehmenskritische Datenströme zu minimieren.

Zielgerichtete Logfile-Analyse

ArcSight Logger bietet ein rollen-basiertes oder personalisiertes Dashboard, welches alle relevanten Reports in einer Konsole vereinigt. Aus diesem zusammenfassenden Dashboard können die Benutzer spezifische Reports ziehen und auch Audit-Workflows nachbilden. ArcSight Logger verwendet in den Reports das ArcSight Common Event Format (CEF). Das hat den grossen Vorteil, dass bei der Auswertung nicht auf spezifisches System- und Logdaten-Know-how zurückgegriffen werden muss. Interessante Reportresultate können mit einem einfachen, google-ähnlichen Interface weiter analysiert werden. Die Suchabfragen können in Echtzeit-Alerts umgewandelt werden, welche ArcSight Logger direkt via SMTP, SNMP oder Syslog an die entsprechende

Stelle weiterleiten kann. Benutzer gelangen via Drill-Down-Menu vom Alert direkt zum entsprechenden Event und können so umgehend das Ereignis untersuchen. Dieser logische Arbeitsfluss zwischen den verschiedenen Funktionen ermöglicht eine effiziente Arbeitsweise.

Performance ohne Kompromisse

Die meisten Log-Management-Produkte unterstützen eine rasche Log-Analyse nur mit Abstrichen bei der Datensammlung und mit Effizienz einbussen bei der Datenspeicherung oder erfordern zusätzliche Hardware. ArcSight Logger bietet eine einheitliche Architektur und minimiert dadurch den Datenaustausch innerhalb der Lösung. So kann ein einziger Logger Rohdaten-Logs mit einer Geschwindigkeit von bis zu 100 000 Events pro Sekunde durchsuchen. Durch die maximale Komprimierung können auf einer einzelnen Logger Appliance bis zu 42 TB Logdaten sicher gespeichert werden.

Skalierbarkeit von kleinen bis zu grossen Unternehmen

ArcSight Logger ist in verschiedenen Performance-Varianten und als Appliance oder Software-Version verfügbar. Diese Lösung ist problemlos linear skalierbar, je nach Datensammlung oder nach Analyse-Performance, je nach Kapazität, die gewünscht ist. Grosse Unternehmen mit separat administrierten Domains oder Service Provider

können ArcSight Logger auch hierarchisch oder peer-to-peer-mässig verteilen. So erhalten Organisationen jederzeit eine unternehmensweite Ansicht sämtlicher Logdaten.

Einfaches Rollout und Management

Für die Bedienung von ArcSight Logger ist kein spezifisches Datenbank-Administratoren-Wissen notwendig. Das GUI ermöglicht 100-%ige webbasierte Administration. Das Rollout und das Management werden so stark vereinfacht und es ist keine Client Installation notwendig. Spezielle Konfigurationen, wie z. B. der ArcSight PCI Logger, werden in einer All-In-One Lösung für Datensammlung, Speicherung und mit einem vorgefertigten Analyse-Paket angeboten. So können auch kleinere Unternehmen mit einem minimalen Aufwand ihre PCI-Initiative starten.

stellt sicher, dass Daten im Fall eines Verbindungsunterbruchs nicht verloren gehen. Weiter bietet ArcSight Logger ein automatisches Failover für die ArcSight Connectors auf eine zentrale ArcSight-Logger-Destination. Die Logdaten werden zuverlässig übermittelt und es wird sichergestellt, dass die Daten unterwegs nicht verändert oder gestohlen werden. Integrity Checks werden nach dem NIST 800-92 Log-Management-Standard durchgeführt.

Neuerungen in der Version ArcSight Logger 4.5

In der neuen Version 4.5 ist der ArcSight Logger erstmals als reine Software-Version verfügbar. Die Software wird in vier verschiedenen Varianten angeboten: «ArcSight Logger 5GB/day» bis «ArcSight Logger 160GB/day». Die Lösung unterstützt folgende Betriebssysteme: Red Hat Enter-



Logfile-Analyse für KMUs!



ArcSight Logger

Sammelt sämtliche Logdaten

- Einfaches Rollout & Management
- Flexible Speicherung
- Logdaten in Audit-Qualität
- Performance ohne Kompromisse

Technische Features

- NEU: als reine Software-Version für LinuxOS erhältlich
- Über 300 Connectors Out-of-the-Box inbegriffen
- SDK zur Integration von Eigenapplikationen verfügbar

Im Rahmen eines Proof of Concept (PoC) installieren wir Ihnen gerne ArcSight Logger.

bw digitronik: Ihr Partner für Informationssicherheit.
Telefon 044 905 48 50
www.bwdigitronik.ch

Flexible Speicherung

ArcSight Logger bietet komplett flexible Speicheroptionen. In Ergänzung zu den vorhandenen Storage RAIDs in den ArcSight Appliances können bestehende NAS-, DAS- oder SAN-Investitionen geschützt und als primärer Datenspeicher genutzt werden. Egal, ob die Daten auf der ArcSight Appliance oder extern gespeichert werden: Die Logdaten werden mit einer Rate von 10:1 effizient komprimiert. Ein rollenbasiertes Zugriffsmodell schützt die System- und die Eventdaten. Zusätzlich können verschiedene Richtlinien erstellt werden, welche entweder auf Regulatorien, Source Typen oder IP-Adressen basieren. Einmal definiert, werden die Richtlinien automatisch ausgebracht, ohne dass ein manueller Arbeitsgang notwendig wird.

Logdaten in Audit-Qualität

Um Logdaten auch für Compliance Audits nutzen zu können, müssen Organisationen nachweisen, dass die Integrität und die Verfügbarkeit der Daten sowohl beim Datenfluss als auch bei der Speicherung voll gewährleistet sind. Verschiedene audit-relevante Controls sind in ArcSight Logger eingebaut. Die ArcSight Connectors unterstützen lokales Caching in Remote Sites. Dieses Feature

prise Linux, CentOS und Oracle Enterprise Linux. Die Hardware-Anforderungen für die kleineren Software-Varianten sind: ein 4-Core-64-Bit-Prozessor (Intel Xeon Quad Core oder ähnlich), 12 GB Memory, 850 GB Speicherplatz und 120 GB Root Partition. Für die grösseren Software-Lösungen wird folgende Hardware empfohlen: zwei 8-Core-64-Bit-Prozessoren, 24 GB Memory, 4.5 TB Speicherplatz und 400 GB Root Partition. Die Version 4.5 bietet zusätzliche «Out-of-the-Box»-Reports und weitere Verbesserungen und Optimierungen. So kann ArcSight Logger auch in kleineren Unternehmen eingesetzt werden.

bw digitronik: Der ArcSight-Partner

bw digitronik ist der ArcSight-Partner in der Schweiz. Wir beraten Sie bei der Konzeption und der Implementierung einer ArcSight-Lösung. Gerne stellen wir Ihnen im Rahmen eines Proof of Concepts die Vorzüge von ArcSight bei Ihnen im Hause vor. Fordern Sie uns heraus! ■



www.bwdigitronik.ch/siem
www.arcsight.com/products/products-logger

Windows 7 und IT-Security

McAfee Endpoint Security macht Windows 7 sicher.

Das Jahr 2010 wird für viele Unternehmen als das Windows-7-Migrationsjahr in die Geschichte eingehen. Wenn man sich an die Migration eines Betriebssystems macht und einen neuen Standard Client definiert, müssen zwingend die Sicherheitsanforderungen gründlich geklärt werden. Windows 7 ist in einer Standard-Installation nicht besonders sicher, da Microsoft an einigen Stellen das Thema Sicherheit dem Benutzerkomfort geopfert hat. Mit einem guten Sicherheitskonzept für den Standard Client, mit McAfee Endpoint Security und einigen durchdachten Sicherheitseinstellungen wird Windows 7 ein sicheres Betriebssystem für Unternehmen.

Sicherheitskonzept für den Standard Client

Allgemein sollte bedacht werden, wie der Standard Client am einfachsten und effizientesten verwaltet werden kann. Es ist für Administratoren hilfreich, wenn Werkzeuge zur zentralen, standardisierten Verwaltung der Clients vorhanden sind. Um bekannte Sicherheitslücken rasch schliessen zu können, ist ein Patch-Management-System notwendig. Das kann für das Windows-Betriebssystem und weitere MS-Applikationen mittels Microsoft Systems Management Server geschehen. Doch Lücken gibt es nicht nur in Microsoft Software, sondern auch in anderer weit verbreiteter Software, wie z.B. Adobe Reader, Flashplayer, Firefox etc. Um diese Produkte auf dem aktuellsten Security-Patch-Level zu halten, bieten sich entweder umfassende Patch-Management-Lösungen an, wie z.B. Lumension Patch and Remediation¹ oder interne Software-Verteilungssysteme.

Um den Standard Client proaktiv vor aktuellen Bedrohungen zu schützen, muss die Möglichkeit bestehen, neue Richtlinien, Signaturen und Updates zentral zu verteilen und entsprechend auf die Clients zu pushen. Die Sicherheitsverantwortlichen benötigen einen sicheren Nachweis, dass die entsprechenden Aktualisierungen ausgebracht und installiert wurden. Hierzu ist ein zentrales Reporting eine wichtige Unterstützung.

Wenn man das Sicherheitskonzept für einen Standard Client ausarbeitet, reicht es nicht aus, nur diesen zu betrachten. Es ist notwendig, sich auch Gedanken über die Netzwerkumgebung zu machen, in welche der Client integriert sein wird. Dazu gehört die Definition der Kriterien für die Zulassung ins Unternehmensnetzwerk sowie die Berücksichtigung der zusätzlichen Herausforderungen bei mobilen Clients.

a) Sicherheit in der Netzwerkumgebung

Jeder Client ist in eine Netzwerkumgebung eingebunden, entweder im internen Netzwerk oder extern. Darum muss der Verbindungsaufbau zum Internet genau definiert werden. Welcher Browser und welche Plug-Ins kommen zum Einsatz und wie wird die Verbindung aufgebaut? Generell muss die Internetverbindung immer über einen Proxy aufgebaut und in ein mehrstufiges Sicherheitskonzept eingebunden werden.

Das heisst, dass z.B. der ein- und ausgehende E-Mail-Traffic zuerst am Gateway überprüft wird², danach auf dem Mailsystem und zu guter Letzt auch noch auf dem Client. Diese Mehrstufigkeit gilt auch für den Web-Verkehr. Zusätzlich sollte der Proxy auch über ein HTTPS-Scanning verfügen, weil sonst die Sicherheitssysteme ausgehebelt werden können und der Client einfacher angreifbar wird.

Für mobile Clients muss ein zusätzliches Sicherheitskonzept für den Internetzugriff definiert werden. Der sicherste Weg ist, dass der Internetzugang für mobile Clients nur via VPN-Umgebung des Unternehmens erlaubt ist und alle weiteren Optionen ins Internet zu gelangen technisch unterbunden werden. So ist auch der externe Client in die Sicherheitsarchitektur des Unternehmens eingebunden, egal, von wo er sich ins Internet einklinkt.

b) Sicherheit auf dem Client

Lange dachte man, dass «die Bösen» nur ausserhalb des Unternehmensnetzwerks lauern (WAN oder www), nicht aber drinnen im LAN. Mittlerweile hat sich die Erkenntnis durchgesetzt, dass es durchaus auch im internen Netzwerk Gefahren für einen Client gibt. Jede Veränderung an den lokalen Einstellungen, die Installation von zusätzlichen Plug-Ins oder neuen Applikati-

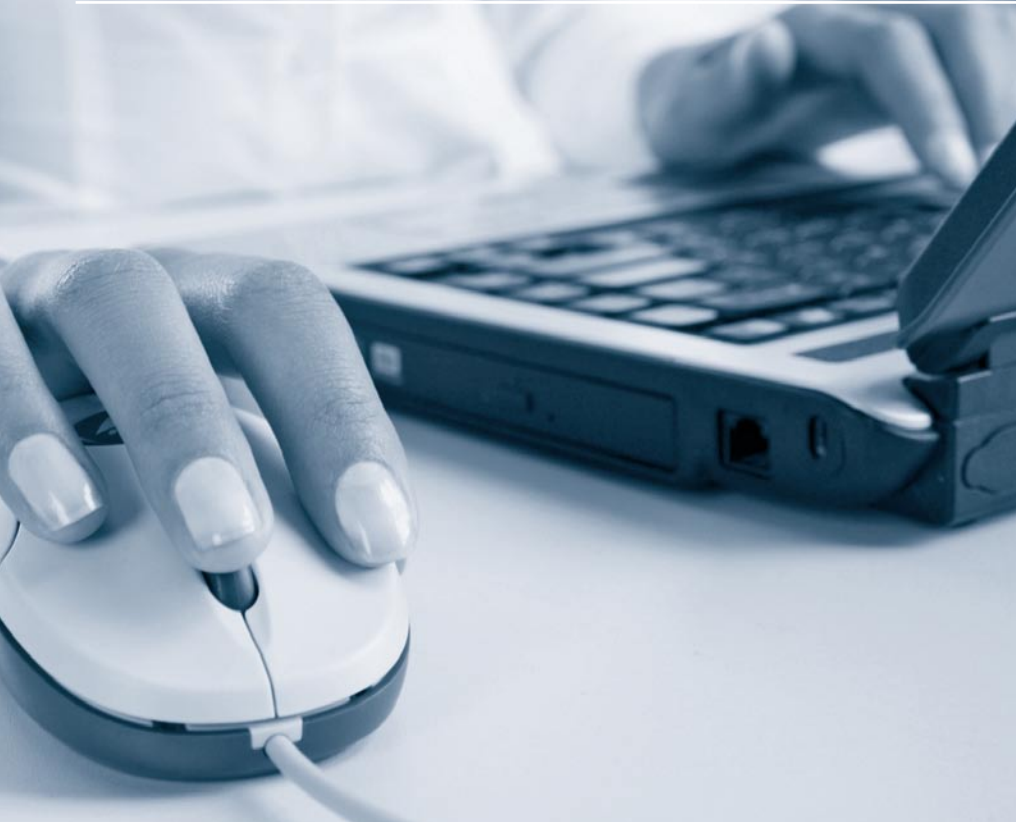
onen verändert die Sicherheitssituation für den Client. Darum sind im Idealfall die lokalen Administratorenrechte nicht zu gewähren. Die Praxis jedoch zeigt, dass dies nicht durchgehend möglich ist, da verschiedene Systeme Administratorenrechte verlangen. Eine Abhilfe können in diesem Fall Application-Control-Lösungen schaffen, wie z.B. Lumension Application Control³. Damit der Client sicher ist, sind folgende Sicherheitskomponenten im Minimum unerlässlich: Malware-Schutz und Device Control. Für mobile Clients ist zusätzlich eine Firewall, kombiniert mit Host-Intrusion-Funktionalitäten und eine Hard-Disk-Encryption notwendig, um optimalen Schutz zu gewährleisten.

Sicherheit mit McAfee Endpoint Security

Natürlich liefert auch Windows 7 ins Betriebssystem integrierte Security Features mit. Doch erfordern diese detailliertes Know-how, um eine annehmbare Sicherheit zu bieten. Und trotzdem sind einige wichtige Möglichkeiten nach wie vor nicht gegeben, wodurch wichtige Sicherheitsanforderungen für Unternehmen nicht vollständig erfüllt werden können.

Um ihren Client mit Windows 7 sicher zu machen, empfiehlt bw digitronik die Komponenten der McAfee Endpoint Security zu verwenden. McAfee zeichnet sich durch einen langjährigen, exklusiven Fokus auf IT-Security aus und hat mit dem Management- und Reporting-Tool ePolicy Orchestrator seit Jahren eine führende Lösung mit zukunftsweisendem Design, in welches kontinuierlich neue Security Komponenten eingebunden werden können, auf dem Markt. Mit einer praxisorientierten Zusammenstellung von bewährten Security-Komponenten in entsprechenden Suites ist es McAfee gelungen, hinsichtlich Beschaffungs- und Wartungskosten sehr attraktiv zu sein.





Den Basisschutz für den Standard Client liefern McAfee VirusScan Enterprise und das Spyware-Modul. Damit ist das Gerät vor Mal- und Spyware sicher geschützt. Der McAfee SiteAdvisor warnt den Benutzer beim Surfen im Internet vor unsicheren Webseiten, indem er zu jeder angesurften Site ein Rating liefert, bzw. für mit Malware verseuchten Seiten den Zugriff ganz blockiert. Zusätzlich können mit dem Host URL Filtering Module nicht erwünschte Webseiten gesperrt werden.

Mit McAfee Device Control werden die verschiedenen Schnittstellen überwacht bzw. die entsprechenden Zugriffsmöglichkeiten gesteuert oder ganz eingeschränkt. So können z.B. USB-Ports oder Laufwerke bei definierten Benutzergruppen selektiv blockiert werden. Weiter kann das Kopieren oder Lesen von Daten über eine Richtlinie gesteuert und im Reporting nachgewiesen werden.

Für mobile Rechner sind die McAfee Desktop Firewall und das Host IPS empfohlen. Damit werden die Zugriffe vom und auf den Client gesteuert und auch nicht-signatur-basierte Attacken dank dem IPS erkannt und geblockt. Um die Daten auf dem Notebook sicher zu transportieren, gibt es McAfee Endpoint Encryption. Die gesamte Harddisk wird verschlüsselt, sodass die Informationen auch bei einem Verlust oder Diebstahl sicher geschützt bleiben und von Dritten nicht verwendet werden können.

Mit dem McAfee ePolicy Orchestrator erhalten System-Administratoren und Sicherheitsverantwortliche ein mächtiges Werkzeug in die Hand. Sämtliche McAfee-Security-Komponenten können zentral von diesem Tool aus verwaltet werden. Sicherheitsrichtlinien werden an einem Ort festgelegt und auf alle Clients verteilt. Ebenso können Patches, Updates und Signaturen rasch und unkompliziert auf jeden Rechner verteilt werden. Über die Reporting-Funktion sind Verantwortliche jederzeit über den aktuellen Stand der Endpoint Security informiert und können bei Bedarf gezielte Aktionen durchführen.

dem neuen Windows arbeiten können, verzichten Microsoft weiterhin auf die Überarbeitung einiger relevanter Einstellungen. Dies geht leider zu Lasten der Sicherheit.

Detaillierte Windows 7 Security Guides sind im Internet zu finden. An dieser Stelle empfiehlt bw digitronik die Sicherheitseinstellungen von Windows 7 genau zu überprüfen und entsprechend den Unternehmensrichtlinien anzupassen.

Fazit

Sie erhalten einen sicheren Standard Client mit Windows 7, wenn Sie die Sicherheitseinstellungen im Betriebssystem sorgfältig konfigurieren und wenn Sie den Client mit McAfee-Endpoint-Security-Komponenten ausrüsten. bw digitronik ist langjähriger und grösster Schweizer McAfee-Elite-Partner und unterstützt Sie gerne bei der Evaluation, Implementierung und Konfiguration der McAfee-Security-Komponenten in Ihren neuen Standard Client. Wir nehmen gerne Ihre Anforderungen in einem persönlichen Gespräch auf und helfen Ihnen, das für Sie passende Lösungspaket zu finden, um Ihr Unternehmen optimal zu schützen. Unsere erfahrenen McAfee Security Engineers unterstützen Sie beim sicheren Einsatz der Technologien. ■

- 1) www.bwdigitronik.ch/vulnmgmt & www.lumension.com
- 2) www.bwdigitronik.ch/contentsecurity
- 3) www.bwdigitronik.ch/endpoint_security
www.lumension.com

Security Audits nach OSSTMM



Messbare Sicherheitsüberprüfungen mit Methode.

Weltweit einziger Standard für:

- Security Audit
- Penetration Testing
- Application Security Audit



Jetzt Ihr persönliches Angebot anfordern!

bw digitronik: Ihr Partner für Informationssicherheit.
Telefon 044 905 48 50

Sicherheitseinstellungen in Windows 7

Windows ist nach wie vor das am weitesten verbreitete Betriebssystem. So bleibt es auch weiterhin das Hauptangriffsziel für Cyberkriminelle. Damit möglichst viele Anwender bequem mit



www.bwdigitronik.ch/maleware_protection
www.mcafee.com

EFG Bank setzt bei Endpoint Security auf Lumension Device Control.



Andreas Meister
Head of Information Security, EFG Bank

Background

EFG Bank ist eine Schweizer Privatbank und gehört zur EFG International. Der Hauptsitz ist in Zürich und der Main Operating Hub in Genf. EFG Bank unterhält weitere Filialen in Europa, im Mittleren Osten, in Asien und in Lateinamerika. Das erste Office wurde 1995 in Zürich eröffnet, und EFG Bank ist mit der Überzeugung angetreten, etwas besser zu machen als der Rest der Finanzindustrie. Der Fokus liegt neben hervorragenden Dienstleistungen auf dem Faktor der menschlichen Beziehungen. Es geht darum, die bestmögliche Lösung für den Kunden zu finden. Die unter EFG International zusammengeschlossenen Privatbanken sind an mehr als 50 Standorten in 30 Ländern tätig und beschäftigen rund 2400 Mitarbeitende. Als wichtiger Arbeitgeber in Genf unterstützt EFG Bank seit 2007 den Genève-Servette Hockey Club als Sponsoring-Partner.

Ausgangslage

Bei EFG Bank war es seit Langem Best Practice, dass der Datenfluss von innen nach aussen kontrolliert wurde. Als vor zwei Jahren der Diebstahl von sensiblen Kundendaten in Liechtenstein grosse Wellen schlug, begann auch EFG Bank gewisse Prozesse zu überdenken. Obwohl der Datenverkehr detailliert kontrolliert wurde, war die Verwendung von portablen Speichermedien möglich. So wurde die Information Security mit der Suche nach einer passenden Lösung beauftragt. Wichtig war, dass die grösseren Auslandsfilialen die Benutzerrechte selbstständig verwalten können, die Richtlinien aber trotzdem zentral gesteuert werden.

Lumension Device Control

EFG Bank hat sich nach einem Evaluationsverfahren für die Lösung Lumension Device Control von bw digitronik entschieden. Andreas Meister, Head of Information Security, fasst es so zusammen: «Ich suchte ein Produkt, das sich einfach in unsere komplizierte Unternehmensstruktur integrieren liess. Dank der Delegation der Admin-Rechte im Active Directory (AD) können wir alle Rechte über die Zugehörigkeit der AD-Gruppen steuern. Ein weiteres Kriterium war die Möglichkeit, kopierte Daten zu loggen und flexible, granulare Zugriffsrechte zu vergeben.»

EFG Bank nutzt hauptsächlich die Funktionalität von Lumension Device Control, mit der sich der ausgehende Datenverkehr kontrollieren lässt. Besonders geschätzt wird der Read-Only-Zugriff auf externe Speichermedien. So können Mitarbeitende einander z.B. Ferienfotos zeigen, ohne dass Daten auf externe Devices gespeichert werden können. «Ich finde es auch beruhigend, dass auf Laptops das WiFi-Interface abgeschaltet werden kann, solange sich das Gerät im Unternehmensnetzwerk befindet», rundet Andreas Meister die genutzten Funktionen ab.

Die technische Inbetriebnahme von Lumension Device Control ist für EFG Bank problemlos verlaufen. Die grösseren Herausforderungen bei solchen Projekten sieht Andreas Meister in der Definition des Konzepts (was soll die Lösung können?), in der Planung (wo wird die Lösung implementiert?) und beim Verfassen der entsprechenden Weisung (wer darf was und was nicht mehr?). bw digitronik hat EFG Bank in diesem Prozess kompetent begleitet.

«Wenn in einem Unternehmen, in dem Mitarbeitende viele Freiheiten haben, plötzlich einige davon eingeschränkt werden sollen,



Dienstleistungen

- Security Consulting:
Konzept für Device Control
- Security Engineering für Device Control

IT-Security Lösungen

- Lumension Device Control, 1200 Nodes
- Lumension PatchLink Scan, 1200 Nodes

muss vorsichtig vorgegangen werden» rät Andreas Meister aus Erfahrung. Wichtig ist eine gute Kommunikation und verständliche Information für die Benutzer über die bestehende Einführung einer Lösung zur Zugriffskontrolle. Dies kann die Akzeptanz einer solchen Lösung rasch erhöhen.

Nutzen für EFG Bank

Aufs Ganze gesehen wurde Lumension Device Control positiv aufgenommen. Mitarbeitende, welche täglich mit hochsensiblen Informationen arbeiten, finden es positiv, dass sie keine Möglichkeit mehr haben, Daten nach aussen zu senden oder zu kopieren. So werden sie in Zukunft nicht verdächtigt, falls ein Vorfall publik werden würde. Aussendienstmitarbeitende schätzen die Funktion, Daten auf mobilen Geräten verschlüsseln zu können. Und die Information Security weiss nun besser, was im Unternehmen abläuft und hat einerseits den Datenfluss besser im Griff und hat andererseits eine Lösung zur Verschlüsselung mobiler Datenträger. Zu guter Letzt wurde Lumension Device Control auch von der Revision positiv gewürdigt. bw digitronik konnte so einen wichtigen Beitrag zur Unternehmenssicherheit von EFG Bank leisten. «Ich bin sehr zufrieden mit bw digitronik: Wir haben einen guten Kontakt, einen einfachen Zugang zum Support und erhalten rasch Antworten», freut sich Andreas Meister. ■



www.bwdigitronik.ch/endpoint_security
www.lumension.com
www.efgbank.com

bw digitronik ist umgezogen. Unsere neue Adresse: Uster West 30, 8610 Uster

bw digitronik hat Anfang August 2010 neue Büroräumlichkeiten in Uster West 30 in Uster bezogen. Im KMU-Park Loren, dem neuen Wohn- und Industriequartier in Uster, haben wir zwei Etagen einer KMU-Box bezogen. Nach über achtzehn Jahren an der Strickstrasse 15, auf dem Areal der Büchi AG, sind wir 300 Meter Luftlinie näher an Zürich heran gerückt.



Mit dem Umzug investiert bw digitronik auch in eine neue, grössere Testumgebung, um einerseits die Support-Services weiter auszubauen und um Kunden anhand von Live-Systemen einen tieferen Einblick in die verschiedenen IT-Security-Lösungen aus unserem Portfolio zu ermöglichen. Weiter wurde eine neue VoIP-

Telefonanlage eingebaut. In Arbeit ist ein Support-Ticketing-System, um Kundenanfragen noch effizienter verarbeiten zu können.

Sie sind herzlich eingeladen, spontan bei uns vorbeizuschauen. Wir freuen uns auf Ihren Besuch!



www.bwdigitronik.ch/contact



**16 Jahre
IT-Security-Erfahrung
(seit 1994).**



**Fallen Ihre User auch auf die perfiden
Psycho-Tricks der Hacker rein?**

**Awareness
Beratung und Schulung.**

**Sensibilisierung des Managements
und der Mitarbeitenden im Umgang mit**

**den Gefahren des
Informationszeitalters.**

bw digitronik: Ihr Partner
für Informationssicherheit.
Telefon 044 905 48 50

Steigern Sie den Nutzen und die Effizienz Ihrer IT-Security-Lösung.

Die IT-Welt ist einem raschen Wandel unterworfen. Neue Technologien, neue Features, neue Versionen jagen einander in immer kürzeren Abständen. Was für die Benutzer neue Möglichkeiten eröffnet und im besten Fall die Arbeit erleichtert, kann für die IT-Security zu Kopfzerbrechen führen.

Einerseits müssen Geschäftsleitungen bewerten, welche technologische Neuerungen tatsächlich dem Kernbusiness des Unternehmens einen Nutzen bringen, andererseits müssen neue Anwenderrichtlinien, allenfalls sogar neue Prozesse, definiert werden. Bevor neue Technologien zum Einsatz kommen, ist auch eine Risikoabschätzung und eine Sicherheitsüberprüfung notwendig, um mögliche Konsequenzen abschätzen zu können. Auf technologischer Ebene müssen von Zeit

zu Zeit die Konfigurationen der IT-Security-Lösungen überprüft und den aktuellen äusseren Gegebenheiten und internen Richtlinien angepasst werden. Neue Features müssen getestet und implementiert werden. Nur so können Sie den vollen Nutzen Ihrer IT-Security-Lösung herausholen und die maximale Sicherheit für Ihr Unternehmen bereitstellen.

Unsere erfahrenen und qualifizierten IT-Security-Spezialisten unterstützen Sie gerne bei all Ihren Fragen rund um die Informationssicherheit: Von der Sicherheitsabklärung über das Konzept zum Review einer Lösung bis zur Implementation der neuen Konfigurationen. Mit uns an Ihrer Seite sind Sie sicher! ■



www.bwdigitronik.ch/engineering



**Testen Sie jetzt
zwei führende Device-
Control-Lösungen!**



- **Umfassendes Device Management**
- **Durchsetzung der Richtlinien**
- **Differenzierte Kontrolle**
- **Einfache Installation**
- **Detaillierte Reports**

Verlangen Sie Ihre persönliche Testlizenz.

bw digitronik: Ihr Partner
für Informationssicherheit.
Telefon 044 905 48 50



ORGANISATION (Security Consulting)

bw digitronik

E - SECURITY IS OUR MISSION

Hauptfunktionen

- Security Audits nach OSSTMM
- Information Security Officer auf Zeit
- Aufbau & Betrieb eines ISMS
- Policy-Überprüfung und -Erstellung
- Security-Konzepte und -Beratung

Kundennutzen

- techn. Sicherheitslevel überprüfen
- temporäre, externe Projektleitung
- zentrale Überwachung, Compliance
- Abgleich mit zu erfüllenden Normen
- Konzepte, die umsetzbar sind



MENSCH (Security Awareness)



- Messen der Sicherheitskultur (TWISK)
- Identifikation der Gefahren
- Web-based Training (WBT)
- Awareness Tools
- Awareness-Schulungen

- Überprüfung, wie Sicherheitspolitik von Mitarbeitern gelebt wird
- Grundlage für Awareness-Schulung
- Benchmarking der Awareness
- Sensibilisierung durch Training



TECHNOLOGIE (Security Solutions)



- Security Information Management
- Security Event Management
- gezielte Datensammlung (Logfiles)
- Logfile-Analysen
- verschiedene Compliance-Packages

- Reduktion von Business Risks
- Korrelation der Unmenge von Daten
- Auswertung & Korrelation von Logs
- unternehmensweite Logfile-Analyse
- Abgleich mit diversen Standards (PCI)



- Content Filtering E-Mail-/Webverkehr
- Spam-Filtering und -Verwaltung
- URL-Blocking/HTTPS Scanning
- benutzerspezifische Filterregeln
- SMTP & WEB Appliance-Lösungen

- Schutz vor unerwünschtem Inhalt
- kein Verlust vertraulicher Daten
- effiziente Abwehr der Spamflut
- erhöhte Produktivität der Mitarbeiter
- Berücksichtigung einzelner User



- Open Source Security for Enterprise
- Ergänzung bestehender Lösungen
- Penetration Testing
- Swiss Security Solutions

- OS-basierte Security-Lösungen
- kundenspezifische Features
- Ethical Hacking
- beste Schweizer Qualität



- sichere Netzwerke und Segmente
- clientlose NAC-Lösung
- unterbruchsfrei im LAN einsetzbar
- signaturlose IPS-Lösung
- einfache Kombination NAC und IPS

- kontrollierter Zugang zum LAN
- einfache Implementierung
- Überwachung Netz und Segmente
- wirksamer und proaktiver Schutz
- Schutz vor Netzwerk-Angriffen



- Vulnerability Management/Assessem.
- Patch Management (Multi-Plattform)
- Device Control (Sticks, Laufwerke...)
- Application Control (Software)
- Verschlüsselung von Devices

- Schwachstellen ausfindig machen
- Schwachstellen rasch beseitigen
- nur definierte Devices im Einsatz
- nur definierte Software im Einsatz
- Schutz vor vertraulichen Daten



- Maleware Protection
- Vulnerability Management
- Endpoint Security
- Intrusion Prevention
- Data Loss Prevention
- Gateway Security: Web/Mail/Firewall

- Schutz vor Viren, Spyware ...
- Risiken definieren & Schutz sichern
- umfassender Arbeitsplatz-Schutz
- hoher Schutz für Netzwerke/Hosts
- Schutz vor (internem) Datenklau
- Perimeter-Netzwerksicherheit



- zentrale Encryption-Plattform
- End-to-End-Encryption (Client)
- Gateway Mail Encryption
- Festplatten/Wechseldatenträger
- Schutz gemeinsamer Files (NetShare)

- Richtlinien- und Schlüsselverwaltung
- Secure Messaging zwischen Clients
- Secure Messaging Gateway
- Schutz von Laptops, Sticks, Handys
- kein unbefugter Zugriff auf Daten



- Network Security Appliances (NSA)
- Enterprise SSL-VPN (Remote Access)
- Gateway Security für KMUs
- Continuous Data Protection
- Secure Wireless Solution

- Multicore-UTM-Lösung
- clientloser, webbasierter Zugriff
- SMTP- und WEB-Content-Filtering
- kontinuierliche Datensicherung
- sicherer Wireless-LAN-Verkehr



- einfaches Secure Messaging
- Side-to-Side Encryption (Gateway)
- optional auch End-to-End Encryption
- Verschlüsselung für BlackBerrys
- Secure Managed File Transfer

- Richtlinien- und Schlüsselverwaltung
- Secure Messaging Gateway
- Secure Messaging zwischen Clients
- geschützte Daten auf BlackBerrys
- sicherer Datenaustausch

bw digitronik

E - SECURITY IS OUR MISSION

- Security Evaluation
- Security Implementation
- Security Review
- Security Support
- Security Training

- Evaluierung diverser Lösungen
- professionelle Umsetzung
- Überprüfung eingesetzter Lösungen
- Wir lassen Sie nicht hängen!
- fundierte Security-Ausbildung