

Die Alarmanlage für IT-Infrastrukturen

Gebäudesicherung mit ausgeklügelten Alarmanlagen und Videoüberwachung, sowie automatischer Alarmierung der Einsatzkräfte, ist für viele Unternehmen selbstverständlich. Doch für die IT-Infrastrukturen der selben Firmen gelten vielfach andere Massstäbe. Was für Gebäude zwingend ist, bleibt bei der IT auf der Strecke.



Der virtuelle Einbruch

Wer kennt sie nicht, die engen Schleusen bei Gebäuden von Banken, Versicherungen und vielen anderen Unternehmen. Vielfach darf man sich als Mitarbeiter oder Besucher nicht ohne Badge im Gebäude oder Areal eines Unternehmens bewegen. Jeder Schritt wird von Kameras überwacht und jeder Zutritt aufgezeichnet.

Der Aufwand ist enorm und trotzdem kommt niemand auf die Idee diesen Schutz plötzlich aufzuheben und die Überwachung einzustellen. Daher ist es aus Sicht des externen Auditors unverständlich, dass nicht die gleichen Anforderungen an die IT-Infrastruktur gestellt werden. Heute ist es schon lange nicht mehr notwendig in das Gebäude, sprich das Rechenzentrum zu gelangen um Manipulationen vorzunehmen oder Daten zu «klauen». Eine Sicherheitslücke genügt vollkommen um mitten in die von Mauern und Schleusen geschützte IT-Infrastruktur einzudringen.

Einbrüche erkennen ist schwierig

Was in der Gebäudesicherheit sofort Alarm auslösen würde, bleibt in der virtuellen Welt vielfach verborgen. Wer kann heute schon mit Sicherheit behaupten, nicht von virtuellen Angriffen betroffen zu sein? Die meisten IT-Organisationen sind dazu nur bedingt in der Lage und erkennen bestenfalls erst nachträglich wieweit sie betroffen wurden.

Unsere Kunden sind besorgt und viele auch daran weitere Massnahmen umzusetzen. Vielfach zwingen sie aber die grosse Komplexität und die fehlenden Ressourcen langsam Vorzugehen, oder verhindern am Ende sogar die Umsetzung. Ein Grossteil der Unternehmen ist daher heute noch nicht in der Lage die virtuellen Einbrüche zu erkennen oder gar zu verhindern.



Was beinhaltet die Alarmanlage?

Wie auch beim Gebäude besteht die Alarmanlage einer IT-Infrastruktur aus einer Zentrale und vielen Sensoren. Als Sensoren dienen sämtliche aktiven Systeme und Applikationen die relevante Informationen zur Verfügung stellen können. Zusätzlich zu den Sensoren kommen alle IT-Sicherheitskomponenten wie AntiVirus-, Firewall- und IDS-Lösungen hinzu, welche in die Zentrale integriert werden müssen. Das Ziel der Zentrale ist es, Informationen zentral zu sammeln und so gut wie möglich zu verdichten. Das heisst, es werden nur die wichtigsten Vorfälle alarmiert, ansonsten sind die IT-Organisationen überfordert.

Ziel ist es den Nutzern möglichst zielgerichtete Informationen zur Verfügung stellen. So kann ein Helpdesk Mitarbeiter anhand eines gut dokumentierten Alarms schnell handeln und ein Problem sofort erkennen, auch ohne alle Details zu verstehen. Wohingegen die Spezialisten der IT-Organisation möglichst frei entscheiden wollen welche Informationen sie benötigen,

um besser zu verstehen wie es um die Sicherheit in ihrem Verantwortungsbereich steht. Dies hat das Ziel, die Zusammenarbeit der IT-Organisation zu verbessern, damit Vorfälle schneller erkannt und abgearbeitet werden können.

Wie soll man beim Bau der Alarmanlage vorgehen?

Schrittweise und in fokussierten Teilbereichen der IT-Infrastruktur. Nur wer schnell Resultate und Nutzen aufzeigen kann hat am Ende Erfolg. Erst wenn die gesamte IT-Organisation den Nutzen sieht werden auch alle mitziehen. Dies gilt auch für die Unternehmensführung, welche natürlich hinter einer zentralen Alarmanlage stehen muss. Vielfach ist dies aber ein Problem, vielleicht braucht es gerade da den Vergleich mit dem Gebäudeschutz um Klarheit zu schaffen. Wer hat schon erlebt, dass der CEO die Schleusen an den Eingängen wieder demontieren lässt, weil noch kein Sicherheitsvorfall bekannt wurde?

Wie erkenne ich den Einbrecher?

Erstens gilt es die Fehlalarme zu minimieren und zweitens den echten Sicherheitsvorfall eindeutig zu erkennen. Was so einfach klingen mag ist in der Praxis schwierig. Der Fokus bei der Einführung einer Alarmanlage muss es also sein, das normale Verhalten der IT-Infrastruktur zu verstehen um dann die tatsächlichen Vorfälle zu erkennen. Wurde der Vorfall richtig erkannt müssen vordefinierte Gegenmassnahmen ausgelöst werden. Nur so ist das Unternehmen in der Lage mit der nötigen Geschwindigkeit zu reagieren. Um diese Prozesse optimal zu gestalten und auf die bestehende IT-Organisation abzustimmen, braucht es die langjährige Erfahrung eines MSS-Anbieters. Er kann mit Hilfe des Kunden diese Arbeit richtig umsetzen.

Wer hilft bei einem Sicherheitsvorfall?

Wo in der realen Welt die Securitas, Polizei oder Sondereinheiten zum Einsatz kommen, wird in der virtuellen Welt ein vergleichbarer Ansatz benötigt. Dabei hat der Staat sicher eine kleinere Rolle und nur Zusammen mit den kommerziellen Anbietern eine Chance die Unternehmen erfolgreich zu schützen. Dies wird dazu führen, dass sich in den nächsten Jahren eine Vielfalt



neuer Services im IT-Sicherheitsmarkt etablieren werden. Die Erkennung, Verhinderung und Bekämpfung von virtuellen Angriffen werden im Mittelpunkt stehen, denn nur wer in diesen drei Bereichen adäquat reagieren kann, ist auch in Zukunft gegen die professionellen Angriffe von aussen und innen geschützt.

Von «Managed Firewall» zu «Managed IT-Security»

Auch innerhalb der Kundenbasis von terreActive ist dieser Trend zu spüren. Immer mehr Kunden suchen eine engere IT-Sicherheitspartnerschaft. Sie erwarten vom MSS-Anbieter nicht nur mehr Knowhow bei den einzelnen Produkten und Technologien, sondern auch einen besseren Überblick über die gesamten IT-Infrastrukturen die sie betreiben. Dies führt bei terreActive zu einem stark wissensbasierten Unternehmen das höchste Ansprüche an seine Mitarbeiter stellen muss. Doch auch innerhalb einer spezialisierten Unternehmung wie terreActive, sind diese Services nur als Teamleistung zu erbringen.

Wer eine IT-Sicherheitspartnerschaft sucht sollte deshalb sicher einmal in Aarau vorbeischaun.



Dieser Artikel ist am 6. April 2009 in der Zeitschrift ICT Kommunikation erschienen.

Kunden-News

Managed Security Services – mehr Sicherheit dank Vier-Augen-Prinzip Success Story mit Aspectra AG



Kaspar Geiser
Managing Director und Mitinhaber
Aspectra AG

Aspectra AG – terreActive AG - eine erfolgreiche Partnerschaft seit 2001.

Seit 8 Jahren betreibt terreActive die IT-Sicherheit von Aspectra, einer Managed Security Services-Kundin der ersten Stunden. Als ein führender Anbieter von Dedicated Hosting-Dienstleistungen hat sich Aspectra auf den Betrieb von Informatik-Lösungen für die höchstmögliche Sicherheit sensibler Daten spezialisiert.

Die wichtigsten Vorteile in unserer Zusammenarbeit sieht Aspectra wie folgt:

- klare Abgrenzung der Verantwortlichkeitsbereiche
- Vier-Augen-Prinzip als Garant für maximale Sicherheit
- Sicherung eines hohen Qualitätsniveaus für die Kunden
- Fokus auf die Kernkompetenzen auf beiden Seiten
- Transfer von Fachkompetenz
- Langfristigkeit der Partnerschaft als Erfolgsfaktor

Kaspar Geiser, Managing Director und Mitinhaber von Aspectra AG: «Die klare Aufgabenteilung und gegenseitige Kontrolle zwischen terreActive und Aspectra ist ein wesentlicher Erfolgsfaktor, um unseren Kunden einen Sicherheitsstandard auf höchstem Niveau anbieten zu können.»

Lesen Sie in der Success Story mehr über:

- Gewaltentrennung als Erfolgsfaktor
- Klar definierte Schnittstellen
- Prozesse werden laufend optimiert

www.terreactive.ch/publikationen

Des Weiteren stehen Ihnen unter angegebenem Link Success Stories zu sourcag und Basler Kantonalbank zur Verfügung.

Weitere Informationen

<http://www.terreactive.ch>
<http://www.aspectra.com>

Neue Angebote

tacLOGHost - der Jüngste unserer Produktfamilie

Sicher haben Sie schon irgendwo und irgendwann von unserem tacLOG gehört oder darüber gelesen. Und leider hat er nicht ganz Ihren Vorstellungen entsprochen: zu teuer, zu komplex ...? Dann haben wir nun mit dem tacLOGHost genau den Richtigen für Sie!

Log-Management steht im Vordergrund:

- Kosten sparen: Lizenzierung pro Appliance mit unlimitierter Anzahl Logclients.
- Normalisierung: Zentrale Speicherung unterschiedlicher Logclients.

- Google your logs: Noch nie war Logdaten-Analyse so schnell.
- Beweissicherung: Durch Speicherung und Schutz der originalen Logdaten.
- Hohe Performance: Empfang von über 15'000 Logmessages pro Sekunde.
- Nachhaltig: Einfache Erweiterung zur umfassenden SEM-Lösung.

Lesen Sie unser Factsheet und Sie erfahren weitere Vorteile und Wissenswertes über den tacLOGHost.



Weitere Informationen

<http://www.terreactive.ch/unserangebot>

Factsheet:

<http://www.terreactive.ch/downloads>

Neue Angebote

Kunden nutzen tacLOG-Schulungen

Seit Herbst 2008 führen wir tacLOG Schulungen bei uns im Hause durch. Dies ermöglicht es unseren Kunden sich 2 Tage, ungestört vom täglichen Business, dem Thema Log-Analyse zu widmen.

Ein Log-Management-Tool vereinfacht die Arbeit. Bis es jedoch soweit ist, müssen Logs integriert und Events kreiert werden. Leider bleibt dafür oft nicht viel Zeit, da der Betrieb nicht stillsteht. Diese Zeit ist zudem oft verstükkelt, was der Erlernung eines neuen Tools / einer neuen Arbeitsweise nicht gerade forderlich ist.

Grundlagen-Schulung bei terreActive

In der 2-tägigen Produktschulung tacLOG lernen unsere Kunden alles was es braucht um tacLOG bedienen zu können. Dies beinhaltet einerseits die Analyse von Log-Daten via Web-GUI, als auch die Integration weiterer Log-Clients sowie die Erstellung von Events. Um nicht nur reine Theorie zu vermitteln, steht eine virtuelle Umgebung zur Verfügung in welcher das Vermittelte vor Ort in der Schulung geübt werden kann. Diese Umgebung hat ausserdem zum Vorteil, dass man weder auf Logs / Firewall-Regeln / ... warten muss noch seine produktive Umgebung beim Üben beschädigen kann. Weitere Vorteile der Schulung bei terreActive – im Gegensatz zu Schulung beim Kunden – sind, dass man einerseits fern vom Alltagsgeschäft ist und andererseits mit anderen Kunden und deren Bedürfnissen in Kontakt kommt.

Teilnehmer Feedback

«Im Ganzen eine sehr tolle, informative Schulung.»

«Danke für den ausführlichen Kurs!»

«Kurs hat genau meine Erwartungen erfüllt.»

«Angenehme Umgebung. Vielen Dank für die Schulung.»



Schulung für Experten

Im Moment ist eine Fortgeschrittenenschulung tacLOG im Aufbau. Diese ist für Kunden gedacht, die weitergehende Anforderungen haben. Der Schwerpunkt dieser Schulung wird auf kontextbasierten Events (Events basierend auf mehreren Logzeilen) und GSM (Graphical Statistics Module: graphische Darstellungen von Loginhalten) liegen. Basierend auf den positiven Kundenfeedbacks zum Format der Grundlagenschulung, wird auch diese Schulung in unseren Räumlichkeiten stattfinden. Da die Thematik komplexer ist, ist geplant diese zusätzlich durch einen individuellen Folgetermin beim Kunden zu ergänzen. So kann optimal auf die individuellen Probleme und Anforderungen eingegangen werden.

Weitere Informationen

www.terreactive.ch/training

Partner

Die neusten Partnerschaften



ch.sun.com

Bei den Lösungen von terreActive kommen die kosteneffizienten SUN x86 Systeme zum Einsatz.

Pressemitteilung

www.terreactive.ch/news



www.ironport.com

terreActive erweitert mit der Cisco Ironport-Partnerschaft die E-Mail Security Palette.



www.zarafa.com

Für das Open Source Exchange Ablöse-Produkt von Zarafa ist terreActive neu Integrationspartner.



www.balabit.com

terreActive macht Beratung und Vertrieb für folgende Produkte aus dem Hause Balabit: syslog-ng, Shell Control Box, syslog-ng Store Box.

Übersicht all unserer Partner

www.terreactive.ch/partner

Next

Folgende Events erwarten Sie
in den nächsten Monaten:



Security Breakfast, 25. Juni 2009
Kursaal, Bern

Thema: **E-Mail Security**
Von A wie AntiSpam bis Z wie Zertifikate

Referenten:

Herr Kabas, Basler Kantonalbank

Herr Urs Rufer, terreActive AG

Herr Jürgen Anthamatten, terreActive AG



**Basler
Kantonalbank**
fair banking

Details zur Veranstaltung

www.terreactive.ch/security-breakfast

security-zone, 23. & 24. September 2009
Papiersaal Sihlcity, Zürich

Als Besucher dieser Veranstaltung können Sie von unserem Know-How als Managed Security Service Anbieter profitieren – besuchen Sie dazu den Workshop «Security as a Service/Outsourcing» oder kommen Sie an unserer Workstation vorbei.

security | zone
PLATTFORM FÜR INFORMATIONSSICHERHEIT

Details zur Veranstaltung

www.security-zone.info



Security Breakfast, 3. November 2009
Park Hotel Hyatt, Zürich

Thema: **Alarmanlagen für IT-Infrastrukturen**

Details ab Sommer

www.terreactive.ch/security-breakfast

Weitere Informationen

www.terreactive.ch/veranstaltungen

Abonnemente

Dieser Newsletter erscheint exklusiv auf dem Internet und kann durch Angabe der E-Mail Adresse kostenlos abonniert werden. Er richtet sich in erster Linie an Kunden, Partner und der Firma terreActive nahe stehende Personen, welche sich über die Geschehnisse rund um terreActive informieren möchten.

Die – auch auszugsweise – Reproduktion, Übersetzung sowie sonstige Verwendung der Inhalte des Newsletters ist nur nach ausdrücklicher Genehmigung durch terreActive AG gestattet.

terreActive AG Kasinostrasse 30 CH-5001 Aarau
www.terreactive.ch

Wir sichern Ihren Erfolg.

terreActive
terreActive
terreActive
terreActive