

In diesem Beitrag:

- Warum es IT-Alarmanlagen braucht
- Die Grundzüge einer IT-Alarmanlage
- Auf Vorfälle reagieren

Die Alarmanlage für IT-Infrastrukturen

Eine Gebäudesicherung mit ausgeklügelten Alarmsystemen, Videoüberwachung und automatischer Alarmierung der Einsatzkräfte ist für Unternehmen heute selbstverständlich. Anders sieht es bei den IT-Infrastrukturen aus. Was für Gebäude zwingend ist, bleibt bei der IT oft auf der Strecke.

Infos zum Autor

**Rolf Hefti**

Head of Marketing & Sales bei Terreactive Schweiz

Wer kennt sie nicht, die engen Schleusen bei Gebäuden von Banken, Versicherungen und unzähligen anderen Unternehmen. Vielfach darf man sich als Mitarbeiter oder Besucher nicht ohne Badge im Gebäude oder Areal eines Konzerns 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

Ansprüche 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 entwenden. Eine einzige Sicherheitslücke genügt bereits, um mitten in die von Mauern und Schleusen geschützte IT-Infrastruktur einzudringen.

Virtuelle Einbrüche erkennen ist schwierig

Was in der Gebäudesicherheit sofort Alarm auslösen würde, bleibt in der virtuellen Welt vielfach verborgen.



gen. Wer kann heute schon mit Sicherheit sagen, nicht von virtuellen Angriffen betroffen zu sein? Die meisten IT-Organisationen sind dazu nur bedingt in der Lage und erkennen bestenfalls erst nachträglich wie stark sie betroffen waren. Vielen Firmen bereitet das natürlich Kopfzerbrechen und sie sind darum bestrebt, wirksame Gegenmassnahmen zu ergreifen. 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 im Stande, die virtuellen Einbrüche zu erkennen beziehungsweise sie zu verhindern.

Was eine IT-Alarmanlage beinhaltet

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 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 wird nur bei den wichtigsten Vorfällen alarmiert, ansonsten sind die IT-Organisationen schnell einmal überfordert.

Ziel ist es, den Nutzern möglichst zielgerichtete Informationen zur Verfügung zu 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 den Zweck, die Zusammenarbeit der IT-Organisation zu verbessern, damit Vorfälle schneller erkannt und abgearbeitet werden können.

Der «Bau» einer IT-Alarmanlage

Beim Aufbau einer Alarmvorrichtung sollte man schrittweise und in fokussierten Teilbereichen der IT-Infrastruktur ans Werk gehen. Nur wer schnell Resultate und Nutzen aufzeigen kann, hat am Ende Erfolg. Erst wenn die gesamte IT-Organisation die Vorteile erkennt, werden auch alle mitziehen. Dies gilt auch für die Unternehmensführung, welche natürlich vorbehaltlos hinter einer zentralen Alarmanlage stehen muss. Oftmals ist aber genau dies ein Problem – vielleicht braucht es gerade in diesem Zusammenhang 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 man «Einbrecher» erkennt

Erstens gilt es, die Fehlalarme zu minimieren und zweitens den echten Sicherheitsvorfall eindeutig zu erkennen. Was so einfach klingen mag, ist in der Praxis nicht trivial. Der Fokus bei der Einführung einer Alarmanlage muss also darauf gerichtet sein, das normale Verhalten der IT-Infrastruktur zu verstehen, um dann die tatsächlichen Vorfälle zu identifizieren. Wurde der Vorfall richtig erkannt, müssen vordefinierte Gegenmassnahmen ausgelöst werden. Nur so ist das Unternehmen in der Lage, mit der notwendigen Geschwindigkeit zu reagieren.

Um diese Prozesse optimal zu gestalten und auf die bestehende IT-Organisation abzustimmen, empfiehlt es sich durchaus, auf die langjährige Erfahrung eines MSS-Anbieters (Managed Security Services) zu setzen. Dieser ist in der Lage, mit Hilfe des Auftraggebers die erforderlichen Massnahmen fachgerecht umzusetzen.

Wer für Sicherheitsvorfälle zuständig ist

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. □

