

IV. Nähere Betrachtung einzelner Angebote

1. Externes Firewall-Monitoring

Die Argumente für eine externe Vergabe der Überwachung von Firewalls sind zunächst bestechend. Auf die Frage, ob es wichtig ist, die Log-Dateien einer Firewall zu überwachen, antwortet die überwiegende Mehrheit der Firewall-Administratoren in Firmen mit „Ja“.

Wenn man weiter fragt, bei welchen Firmen diese Logs tatsächlich täglich oder auch nur wöchentlich analysiert werden, so findet man nur noch eine kleine Minderheit.

Outsourcing-Anbieter wollen hier helfen, indem die Logs der Firewalls von einem Tag und Nacht besetzten SOC überwacht werden.

Um die Kunden noch weiter zu überzeugen, vergleichen sie gelegentlich Firewalls mit feuerfesten Safes, die im Brandfall ihren Inhalt auch nur für eine bestimmte Zeit sichern. Auch Firewalls – so wird argumentiert – schützen nur für eine bestimmte Zeit gegen Hacker. Irgendwann müsste man Gegenmaßnahmen einleiten oder der Hacker würde erfolgreich sein.

Betrachtet man die tatsächlichen technischen Möglichkeiten einer Firewall, sowohl von der Schutz-Seite, als auch von Seite der Logs, so muss man die Verkaufsargumente der Anbieter teilweise in Frage stellen.

Die erste wichtige Frage ist, was in den Log-Dateien einer Firewall überhaupt zu sehen ist und was damit eigentlich überwacht werden kann. Eine typische Firewall besitzt eine Policy, in der definiert ist, was erlaubt ist und was nicht. Pakete oder Verbindungsanforderungen, die nicht erlaubt sind, werden blockiert und erzeugen einen Eintrag in der Log-Datei. Ein ungeschickter Angreifer, der eher unmotiviert und blind versucht auf verschiedenste Dienste zuzugreifen, wird viele Einträge im Log verursachen. Ein erfahrener Hacker dagegen kann die Firewall unbemerkt erkennen und mögliche Angriffspunkte ausfindig machen, ohne dass er selbst im Log der Firewall erscheint. Falls er eine Verwundbarkeit innerhalb eines erlaubten Protokolls oder Dienstes findet, so kann er ebenfalls einbrechen, ohne dass die Firewall davon etwas merkt. Der Grund dafür ist weniger das Geschick des Hackers, sondern vielmehr eine Grundeigenschaft von Firewalls.

Firewalls verbieten oder erlauben bestimmte Kommunikationsprotokolle. Sie sind aber zur Erkennung von Angriffen nur sehr wenig geeignet.

Für ein externes Firewall-Überwachungs-Center gelten diese Einschränkungen auch.

Erfolgreiche Angriffe können in den seltensten Fällen bemerkt werden. Nur einfache und erfolglose Angriffe, die als Nebeneffekt viele Log-Einträge erzeugen werden erkannt.

Die zweite Frage, die sich daran sofort anschließt ist, welche Reaktionen ein externer Überwachungs-Dienst auslösen kann und sollte. Die wichtigste Reaktion bei einem erfolgreichen Angriff wäre den Schaden zu begrenzen, die Schwachstelle ausfindig zu machen, aufgrund der Einbruch möglich wurde und den Angreifer zu lokalisieren. Da aber schon die Erkennung eines erfolgreichen Angriffs mit einer Firewall-Überwachung alleine nicht möglich ist, kann auch die Eskalation nur begrenzt erfolgreich sein. Unabhängig davon muss die Einbruchsanalyse meist vor Ort erfolgen.

Stattdessen müssen die externen Überwacher aber aufgrund des Vertrages auf ungeschickte Angriffsversuche reagieren. Falls diese Versuche offensichtlich sind, wird die Quelladresse des Angriffs meist notiert und im nächsten Bericht an den Kunden als Rechtfertigung des Überwachungs-Dienstes präsentiert. Falls sogar aktives Eingreifen in die Firewall-Policy des Kunden vereinbart wurde, kommt es auch vor, dass „zum Schutz“ sämtliche Kommunikation von der Quelladresse des Angreifers blockiert wird.

Da kein halbwegs intelligenter Hacker von seiner eigenen Adresse aus angreift, sondern zunächst über verschiedene Schritte und bereits andere geknackte Server seine Herkunft verschleiert, führt diese neue Firewall-Policy lediglich dazu, dass der Angreifer bemerkt, dass er entdeckt wurde. Er kann nun etwas vorsichtiger und von einer anderen IP-Adresse aus weitermachen.

Ein weiterer interessanter Punkt ist die Überwachung von Systemen durch qualifiziertes Personal: Viele Anbieter werben damit, dass die sicherheitsrelevanten Informationen – vor allem Log-Daten – rund um die Uhr von Spezialisten ausgewertet werden. Wer in seinem Unternehmen selbst Schichtdienst und Rufbereitschaften kennt, wird bestätigen, dass gerade die hochqualifizierten IT-Spezialisten – und zu dieser Gruppe zählen Sicherheitsfachleute zweifelsohne – kaum dazu zu bewegen sind, in der Nacht in einem Operating Center Logs zu verfolgen. Stattdessen werden diese Jobs vor allem von Berufseinsteigern oder Umsteigern besetzt, die von dort zu einem Berater-Job zu normalen Arbeitszeiten befördert werden wollen. Auch bei Firmen, die Firewall-Überwachung anbieten, arbeiten häufig keine anderen Leute. Sie werden durch automatische Filter unterstützt, die uninteressante Log-Einträge ausblenden sollen, damit „Angriffe“ besser erkannt werden können.

Zusammengefasst kann man sagen, dass die ständige Überwachung von Firewalls, zur Erkennung von Angriffen und zur rechtzeitigen Reaktion kein besonders sinnvolles Unterfangen ist. Unabhängig davon kann eine Überwachung mit anderen Zielen durchaus sinnvoll sein. Beispielsweise könnte die Verfügbarkeit, der Datendurchsatz oder die CPU-Auslastung überwacht werden, um bei Ausfall schnell einschreiten zu können.

2. Externes IDS-Monitoring

Im Gegensatz zu den bisher diskutierten Firewalls ist ein Intrusion Detection System (IDS) dafür entwickelt worden, Angriffe zu erkennen. Der Sinn eines IDS liegt ja sogar primär in der Erkennung und Alarmierung und nicht wie bei einer Firewall in der Zugriffskontrolle. Die Überwachung eines IDS ist damit eine offensichtlich sinnvollere Aufgabe als die Überwachung von Firewall-Logs. Ohne eine Überwachung und Reaktion auf die Alarme beim Betrieb wäre das IDS sogar völlig nutzlos.

Der zweite und neben der Überwachung mindestens ebenso wichtige Aspekt ist die Eskalationsprozedur. Eine Überwachung rund um die Uhr ist nur dann sinnvoll, wenn im Fall eines erkannten Einbruches auch in der Nacht richtig reagiert werden kann. Genau dieser Teil stellt eine externe Überwachung jedoch vor Probleme, denn eine Reaktion auf einen Einbruch in einen internen Server erfordert interne Reaktionen, die nur in Absprache und mit Unterstützung der internen IT-Abteilung durchgeführt werden können. Die einzigen Teilaufgaben, die extern erledigt werden könnten, sind die Beobachtung und gegebenenfalls Rückverfolgung des Angreifers.

Eine externe Überwachung von IDS-Alarmen ist damit durchaus sinnvoll. Die Einbettung in bestehende Organisationsstrukturen, interne Abläufe und Verantwortlichkeiten speziell in Hinblick auf die Reaktion bei einem Angriff ist jedoch eine wesentliche Voraussetzung, die vor einer Entscheidung über Outsourcing gut überlegt sein sollte.

3. Externes Firewall-Management

Die Angebote für externes Firewall-Management sind vielfältig. Sie unterscheiden sich jedoch vom externen Monitoring vor allem durch die aktive Einflussnahme des Outsourcing Anbieters. Teilweise enthalten Firewall-Management-Angebote auch die Überwachung und manchmal gehören die Firewall-Komponenten, die beim Kunden stehen sogar dem Outsourcing-Anbieter. Meist wird dem Kunden jedoch eine Auswahl der folgenden Tätigkeitsbereiche angeboten:

- **Systempflege in Bezug auf Backups, Plattenplatz etc.**
- **Reparaturen oder Hardware-Austausch sofern nötig**
- **Einspielen von Software-Updates und Patches sofern nötig**
- **Konfiguration der Regelbasis nach Anforderung des Kunden**

Speziell die ersten Punkte sind sicher dankbare Aufgaben, die sich durchaus von einem externen Outsourcing Anbieter erledigen lassen. Selbstverständlich müssen auch dabei interne organisatorische Prozesse berücksichtigt werden. Die Konfiguration der Regelbasis jedoch ist je nach Anwendungsbereich der Firewall extern nicht unbedingt sinnvoll machbar. Es kommt dabei vor allem darauf an, ob die Firewall-Regelbasis relativ fix ist oder ob sie ständigen Änderungen unterworfen ist. Eine Remote-Access-Firewall in einer großen Firma beispielsweise, die den Support-Zugang für viele wechselnde externe Partner verwaltet, wird weniger geeignet sein, da vor allem neue Benutzer angelegt werden müssen, die bestimmten Gruppen zugeordnet werden. Der Aufwand für die technische Umsetzung dieses Vorgangs ist sehr gering aber der Overhead, um jeden dieser Vorgänge an einen externen Outsourcer zu übergeben, der natürlich wieder prüfen muss, ob die Anforderung berechtigt ist, übersteigt teilweise den Aufwand der Durchführung.

4. Externes Management von IDS

Ähnlich wie beim externen Firewall-Management ist der Schwerpunkt bei IDS-Management die Systempflege, Hardware- und Software-Updates. Häufige Änderungen einer Regelbasis gibt es bei IDS-Sensoren nicht, stattdessen aber ein Feintuning der Erkennungsrate und eine ständige Aktualisierung von Signatur-Datenbanken, damit auch neue Angriffe erkannt werden können.

Inhaltlich können diese Aufgaben durchaus extern durchgeführt werden. Es ist eher eine organisatorische und auch kaufmännische Frage, ob es sich lohnt, diese Aufgaben extern zu vergeben.

5. Externe Firewalls beim ISP

Wer bereits darüber nachdenkt, eine Firewall nicht nur extern überwachen, sondern sie auch extern betreiben zu lassen, der wird sich auch fragen, warum er überhaupt noch Hard- und Software bei sich aufbauen soll. Eine Alternative dazu ist, eine Firewall bei einem externen Partner zu nutzen und selbst nur noch eine dedizierte Leitung zu diesem Partner zu halten. In der Realität wird dies vor allem von Internet Providern angeboten. Der Kunde kauft dabei keinen einfachen Internet-Anschluß, sondern eine Leitung, die beim Provider über eine Firewall ins Internet geht.

Technisch realisiert der Provider dieses Szenario meist über „virtuelle“ Firewalls bzw. über eine große zentrale Firewall, die für jeden Kunden eine eigene Policy abbilden kann. Gerade für kleine Firmen ist diese Variante durchaus interessant.

Die Gegenargumente sind die häufig fehlende Flexibilität hinsichtlich der Struktur und Funktionen der Firewall, sowie die maximale Abhängigkeit von den Providern, die dadurch entsteht.

Für große Firmen, die womöglich sogar mehrere redundante Internet-Anschlüsse benötigen, ist dieses Modell keine Option.



cirosec GmbH
Ferdinand-Braun-Straße 3
74074 Heilbronn
Tel.: 07131 / 59455-60
Fax: 07131 / 59455-99
www.cirosec.de

6. Externe Virens Scanner-Gateways

Ebenso, wie man über externe Firewalls bei einem Provider nachdenken kann, ist es nahe liegend, auch Virens Scanner-Gateways für E-Mails oder für Web-Zugriffe extern zu nutzen. Im Fall von E-Mails werden eingehende Mails nicht mehr direkt zum Kunden geschickt, sondern zunächst an ein Relay des externen Anbieters. Dort werden die Mails nach Viren durchsucht und erst nach erfolgreicher Prüfung an den Kunden weitergeleitet. Der externe Anbieter sorgt vor allem dafür, daß der Scanner immer verfügbar ist und daß die aktuellsten Virus-Signaturen eingespielt sind. Bei völlig neuen Viren, die von den Scanner-Herstellern noch nicht erkannt werden können, wäre auch ein manuelles Eingreifen des Anbieters denkbar, bei dem bestimmte angehängte Dateinamen blockiert werden. Für Web- oder FTP-Downloads könnte der Kunde alle Aktivitäten über einen zentralen Proxy des Anbieters schleusen, wo die übertragenen Dateien wiederum nach Viren durchsucht werden.

Typische Kritikpunkte sind Fragen des Datenschutzes, der Verfügbarkeit oder die Möglichkeit, solche Systeme zu umgehen. Speziell wenn alle Mails und Web-Zugriffe über ein zentrales System eines Anbieters gehen, entstehen dort auch Log-Informationen über das detaillierte Benutzerverhalten der Mitarbeiter des Kunden.

Von der technischen Seite betrachtet ist ein solcher Dienst eine sehr einfache Sache. Er erfordert auch auf der Anbieter-Seite kaum Personal. Dementsprechend stellt sich natürlich auch bei den Kunden die Frage, ob man durch geschickte automatische Signatur-Updates nicht dasselbe Ergebnis erreichen kann und ob der Personalaufwand in diesem speziellen Fall nicht so gering ist, dass sich die eigene Anschaffung eines Virenschutz-Gateways gegenüber einem externen Service schon nach dem ersten Jahr amortisiert hat.

7. Externe Sicherheits-Informationendienste

Das Paradebeispiel für diesen Bereich ist der Anbieter SecurityFocus und ähnliche Dienste. Der Kunde bekommt dort Informationen über neu bekannt gewordene Schwachstellen oder Exploits in Software-Produkten, die ihn interessieren. Gegen Zahlung einer jährlichen Gebühr kann man Accounts im zentralen Online-System des Anbieters definieren. Für jeden Account können dann eigene Interessensgebiete und Filterlisten angelegt werden, so dass jeder betroffene Mitarbeiter nur noch die Meldungen über Schwachstellen bekommt, die für ihn wichtig sind.

Ob man derartige Dienste überhaupt unter dem Titel Outsourcing betrachten möchte ist fragwürdig. Zu dem in der Branche verwendeten Begriff Managed Service paßt es jedoch recht gut, da die Kunden sich bisher selbst um den Bezug von Informationen über Gefährdungen kümmern mußten und dieser Service nicht nur die Lieferung, sondern auch die kritische Aufgabe der Vorfilterung übernimmt.

Argumente gegen einen solchen Service gibt es kaum, allenfalls die übliche Frage, ob der Preis für den gelieferten Service angemessen ist.

8. Automatisierte Scan Services

Sicherheitsüberprüfungen gibt es vielen verschiedenen Ausprägungen mit verschiedenen Schwerpunkten und Ansätzen. Ein etablierter Bestandteil technischer Sicherheitsüberprüfungen von Netzwerken und Servern sind Scans mit Werkzeugen wie Nessus, NMap oder kommerziellen Produkten von ISS, eEye und anderen.

Der Scanner sucht dabei automatisch in einem vorgegebenen Bereich nach Systemen, Diensten und bekannten Schwachstellen. Die manuelle Nacharbeit von externen Beratern oder eigenen Mitarbeitern beschränkt sich meist auf eine Plausibilitätsprüfung und abschließende Bewertung der Scan-Ergebnisse.

Es verwundert daher nicht, daß eine Reihe von Anbietern diesen Dienst als automatischen



cirosec GmbH
Ferdinand-Braun-Straße 3
74074 Heilbronn
Tel.: 07131 / 59455-60
Fax: 07131 / 59455-99
www.cirosec.de

Managed Service anbieten. Der Kunde zahlt dabei wieder einen jährlichen Betrag an den Anbieter und bekommt dafür einen Account auf dem Online-Scan-System des Anbieters. Dort definiert der Kunde die zu scannenden Adressen und Intervalle. Im typischen Fall läuft der Scanner dann jede Nacht und berichtet dem Kunden jeden Morgen in einer E-Mail über Veränderungen bzw. neu gefundene Schwachstellen in den externen Zugängen des Kunden.

Da der Scan-Dienst aus dem Internet auch nur extern sichtbare Adressen überprüfen kann, sind Aussagen natürlich nur für die Perimeter-Sicherheit und nicht für die Sicherheit interner Systeme gültig. Es gibt zwar auch schon Angebote, bei denen ein Scan-Agent in Form einer Appliance in das interne Netz des Kunden gestellt wird, jedoch tun sich speziell Kunden in Deutschland sehr schwer damit, einer solchen Lösung zu vertrauen. Schließlich werden aktuellste Informationen über interne Schwachstellen auf einem externen System eines meist ausländischen Anbieters gespeichert. Dieser Kritikpunkt gilt teilweise auch schon für externe Schwachstellen. Auch hier sollte man prüfen, ob die Daten über externe Schwachstellen bei dem Anbieter wirklich sicher aufgehoben sind.

Generell sind solche externen Scan-Services eine sehr sinnvolle Sache. Die Qualität hängt maßgeblich von der Qualität und Aktualität der eingesetzten Scan-Mechanismen ab. Der Kunde sollte sich hier bei der Auswahl sehr genau informieren und mehrere Angebote vergleichen.

Je nach Anzahl der extern sichtbaren Server ist ein automatischer Scan-Service sogar preiswerter, als eine zweimal im Jahr durchgeführte externe Sicherheitsüberprüfung, bei der auch nur gescannt wird. Der Mehrwert einer manuellen Sicherheitsüberprüfung durch ein Beratungsunternehmen ist nur noch dann gegeben, wenn das Beratungsunternehmen deutlich mehr Prüfungen durchführt als bloßes Scannen. Sinnvolle manuelle Ergänzungen gibt es jedoch genügend, angefangen von der Detailbetrachtung der Konfigurationen und Härten bis zur Sicherheitsanalyse der Applikationen selbst.

V. Generelle Probleme von SOCs

Einige Probleme gelten generell für alle bisher beschriebenen Services.

Der Kunde gibt bei einem Managed-Security-Dienst einen Teil seiner Sicherheitsfunktionen an einen externen Anbieter. Damit ist offensichtlich, dass eventuelle Unzulänglichkeiten oder Schwachstellen in der Sicherheit des Anbieters auch die Sicherheit seiner Kunden beeinflussen. Derartige Schwachstellen sind an vielen Stellen möglich. Die wichtigsten Fragen dabei sind:

- Wie sicher ist das „Secure Operating Center“ des Anbieters wirklich?
- Wie wird die Qualifikation und Erfahrung des Personals im SOC sichergestellt?
- Wie vertrauenswürdig ist dieses Personal?
- Liegen Berichte von Überprüfungen der SOCs und seiner technischen Einrichtungen durch Dritte vor?
- Falls im SOC oder beim Kunden spezielle Hard- und Software zum Einsatz kommt: Ist diese durch aussagekräftige Verfahren auf Ihre Sicherheit geprüft worden?
- Wie sicher ist die Anbindung des SOC ans Internet? Gibt es externe Prüfungen?
- Was passiert im Fall eines Ausfalls des SOC, beispielsweise aufgrund von DoS Angriffen?

Gerade die Sicherheit eines Überwachungs-Centers weicht in der Realität gelegentlich stark von den Marketing- und Vertriebsversprechungen der Anbieter ab. Um hier die Spreu vom Weizen zu trennen, sollte man als Kunde sehr genau hinsehen. Oft glaubt man, Firewall-Experten, die sogar die Firewalls für Kunden überwachen, haben selbstverständlich eine sichere eigene Umgebung. Eine aktuelle externe Sicherheitsüberprüfung durch anerkannte und unabhängige Dritte hilft hier weiter. Als Kunde sollte man nach den schriftlichen Ergebnissen bzw. der Zertifizierung fragen. Liegt so etwas nicht vor oder darf es nicht her-

ausgegeben werden, so ist dies ein erster Grund, misstrauisch zu werden. Falls Überprüfungsergebnisse vorliegen, so ist es auch interessant, welche Aspekte der Sicherheit überhaupt geprüft wurden. Eine funktionierende Feuerlöschanlage und eine hoch verfügbare eigene Firewall helfen nicht weiter, wenn das SOC eine Web-Anwendung zur Kommunikation mit den Kunden nutzt, über die auch Hacker einbrechen können.

V. Zusammenfassung

Bei klassischen Outsourcing Projekten steht primär die Kostenfrage im Mittelpunkt. Dieser Aspekt alleine reicht bei Sicherheits-Outsourcing nicht aus. Die Überwachung oder der Betrieb einzelner Komponenten kann extern vergeben werden. Die Verantwortung für die Sicherheit und eventuelle Einbrüche jedoch nicht. Oft ist dies zwar das Verständnis eines Kunden gegenüber dem externen Anbieter, aber tatsächlich werden genau die kritischen Punkte in den Service-Verträgen meist wieder auf den Kunden abgewälzt.

Man muss daher selbst bewerten, in wie weit die Überwachung und der Betrieb einer Sicherheitsinfrastruktur tatsächlich zu Einsparungen und / oder zu einer höheren Sicherheit führt.

Wie am Beispiel der Firewall-Überwachung diskutiert wurde, gibt es durchaus Angebote, deren Sinn vom Grundsatz her fragwürdig ist. Wenn ein Dienst inhaltlich sinnvoll und vom Preis interessant ist, bleibt die Frage nach der tatsächlichen Sicherheit, die der Anbieter aufgrund seiner eigenen potentiellen Schwachstellen erreichen kann.



cirosec GmbH
Ferdinand-Braun-Straße 3
74074 Heilbronn
Tel.: 07131 / 59455-60
Fax: 07131 / 59455-99
www.cirosec.de