

Außengrenzen sichern

Autor - T. Brake

Außengrenzen Sichern

Roter Faden zur Abwehr von Angriffen

- 1 Sicherung der Außengrenzen Ihres Unternehmens
 - 2 Sicherung der Innengrenzen Ihres Unternehmens
 - 3 Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen
 - 4 Training der Risiko-Erkennung bei für Ihr Unternehmen tätigen Person
 - 5 Betrieb Ihrer zentralen Unternehmens-IT in professionellem Umfeld
 - 6 Betrieb Ihrer Arbeitsplätze auf Grundlage von Desktop-Management
 - 7 Ordnung in den Berechtigungen Zutritt und Zugang herstellen
 - 8 Notfall-Ersatz für die IT-Administration ermöglichen
 - 9 Abschaffen der Praxis „Dateianlagen an E-Mail“ an den Arbeitsplätzen
-

Wer ist für Schutz und Abwehr zuständig?

Als Unternehmer, als Geschäftsführer und auch als Entscheider haben Sie die Verantwortung, die Werte Ihres Unternehmens zu schützen.

Diese Aufgabe nimmt heutzutage den gleichen Wert ein wie beispielsweise Wachstum, Ertrag und Management. Die Aufgabe ist nicht delegierbar und Sie sind – je nach Art und Bedeutung Ihres Unternehmens – persönlich haftbar!

Wer sind denn diese Angreifer?

Angreifer sind heutzutage längst keine Einzelpersonen mehr, sondern bandenartig tätige Gruppen, die gegen „Honorar“ regelrecht beauftragt werden, bestimmte „Aufgaben zu erledigen“.

Welche Unternehmen werden denn angegriffen?

Jedes Unternehmen steht im Wettbewerb zu anderen Unternehmen, und je nach Marktposition, gerät Ihr Unternehmen irgendwann in den Fokus von Angreifern. Es spielt keine wesentliche Rolle, welche Größe Ihr Unternehmen hat. Solange es finanzielle Mittel besitzt, die man beispielsweise erpressen kann, lohnt sich der Angriff. Auch das Vorhandensein fähiger Mitarbeiter könnte Ihr Unternehmen in den Fokus von Angreifern bringen, denn solche Personen werden in unserer modernen Wirtschaft längst als wertvolle Ressource gehandelt.

Außengrenzen Sichern

Wie muss ich mir einen Angriff vorstellen?

Angriffe „von außen“ sind hier das bevorzugte Mittel krimineller Banden. In erster Linie also über das Internet, jedoch auch über W-LAN oder den simplen Zugang zu den Geschäftsräumen oder zur Produktionsstätte, in denen der Großteil der unternehmerischen Wertschöpfung erfolgt. Leider sind Angriffe „aus dem inneren“ durch eigene Mitarbeiter oder Lieferanten überhaupt keine Seltenheit. Diese Art von Angriffen führen in schlimmsten Fällen zu Sabotage, Spionage oder sogar die Unterwanderung durch die Konkurrenz. Hier stehen Zerstörung der Netzwerk-Verkabelung, die Verhinderung der Stromversorgung und die Zerstörung oder Beschädigung Geräte im Serverraum ganz oben auf der Rangliste der Angriffe.

Welche Folgen kann ein Angriff haben?

Bedenken Sie, dass Ihr Unternehmen durch einen Angriff einfach komplett lahmgelegt werden kann. Leider kann es sogar zum Ende Ihres Unternehmens kommen, denn unterschiedlichste Angriffserfolge sind in der Lage, die Betriebsfähigkeit tagelang, manchmal auch über Wochen, lahmzulegen.

Sicherung der Außengrenzen Ihres Unternehmens

Die Außengrenzen Ihres Unternehmens sind eine primäre Angriffsfläche. Diese Angriffsfläche wird als Einstieg in die unterschiedlichen Aktivitäten von Angreifern einbezogen.

Werden die Außengrenzen vom Angreifer überwunden und er ist „nach innen“ gelangt, ist der Angreifer kaum noch zu stoppen!

Der Universal-Schutz ...

... gegen alle Angriffsformen gilt für Unternehmen eine klare und wesentliche Hauptregel: Die Angriffsfläche so klein wie möglich halten!

Außengrenzen Sichern

Dabei ist zu beachten, dass ...

... der sogenannte „Perimeterschutz“ eine wirklich komplexe Angelegenheit ist. Es gibt eine große Menge an empfohlenen Maßnahmen, jede mit eigener Schutzwirkung und unterschiedlichen Kosten in Aufwand und Technik. Doch nicht jede Empfehlung ist angemessen, und nicht jede Maßnahme ist wirksam. Hier hilft nur eine Bewertung durch einen Fachmann, der für das Unternehmen individuell einen Katalog von Maßnahmen erstellt, denn die richtigen Maßnahmen hängen komplett vom Unternehmen ab.

Es ist wichtig zu verstehen, dass ...

... jedes Unternehmen physische Außengrenzen besitzt, und zwar Betriebsstätten, Gebäude, Räume, Homeoffice (u.ä.). Zusätzlich gibt es jedoch noch die besonderen Außengrenzen, die durch Anwendungen (Software), Geräte (Firewall, IP-Modem), das IP-Netzwerk und die Aktivitäten des Unternehmens im Internet gebildet werden. Genau genommen ist jeweils jede beschäftigte Person für sich genommen auch eine „Außengrenze“, z.B. im Privatleben. Auch jede E-Mail, die Dateianlagen mit unverschlüsselten Inhalten transportiert, befindet sich während der Reise durch das Internet im Bereich der Außengrenzen.

Man muss sich klar machen, dass ...

... es hierbei um ganz konkrete Gefahren geht, und die Angriffsformen sowie die Ziele vielschichtig sind:

- **Sabotage**, die zur Betriebsunterbrechung führt
- **Spionage**, die geheime Informationen zum Ziel hat
- **Diebstahl von Daten**, um diese zu verkaufen oder zu nutzen
- **Übernahme**, z.B. von Servern oder Arbeitsplätzen für ein BOT-Net
- **Diebstahl von Identitäten**, um in anderer Identität kriminelle Handlungen durchzuführen.

Außengrenzen Sichern

Folgende 7 Aktionen verkleinern die Angriffsfläche!

In den folgenden 7 Schritten erreichen Sie es, die Angriffsfläche klein zu halten. Die Außengrenzen werden gesichert, wodurch Ihr Unternehmen gegen gängige Angriffsmethoden wirksame Resilienz gegen Angriffe auf die Außengrenzen aufbaut:

1. Betriebsstätte und Unternehmensräumlichkeiten absichern

Problem: Wenn jemand die physischen Außengrenzen überwindet, hat er sich einen Zugang zu der Innenwelt Ihres Unternehmens verschafft.

Lösung: Identifizieren Sie vorhandene physische „offene Türen“ in Ihrem Betrieb. Machen Sie sich eine Liste, und überlegen bei jeder „offenen Tür“, welchen Schaden es anrichten könnte, wenn ein Angreifer diesen Weg nach innen nutzen würde.

Tipp: Arbeiten Sie jeden Punkt auf Ihrer Liste an und schließen nach und nach jede „offene Tür“ durch wirksame Mechanismen (z.B. elektronische Schlösser, Sabotageschutz, Alarmanlagen). Wiederholen Sie dies einmal im Jahr.

Society-Produkt: Mit dem ‚ISM-Code‘ erhalten Sie vom erfahrenen Berater einen Überblick über alle „offenen Türen“ und eine Empfehlung, welcher Schutz angemessen und wirksam ist.

Außengrenzen Sichern

2. Schützen Sie die Internet-Versorgung

Problem: Mit dem Internet sind zwei Gefahren verbunden, die Sie beachten müssen.

Die erste Gefahr besteht darin, dass die Anbindung ausfällt und Ihr Unternehmen von der Kommunikation abgeschnitten wird. Das kann durch

- **Sabotage** (Seitenschneider, Bagger) oder
- **Ausfall des Providers** (Störung, Übergabepunkt ausgefallen) oder
- **Ausfall der Firewall** (Gerät defekt oder fehlerhafter Bedienung) geschehen.

Lösung: Zuerst schaffen Sie einen zweiten „Internetanschluss“ bei einem anderen Provider an, auf den umgeschaltet wird, wenn die eigentliche Anbindung ausfällt. Betreiben Sie die Firewall zusammen mit einem Zweitgerät, welches sich aktiviert, wenn das Hauptgerät aus irgendeinem Grund versagt.

Society-Produkt: Mit Society Ocean™ ‚Pier‘ erhalten Sie zusammen mit der Serviceleistung Managed-Security die zu Ihnen passenden Firewall-Geräte.

3. Schützen Sie Ihr lokales Netzwerk (LAN)

Problem: Die Kommunikation im LAN ist üblicherweise vollkommen vertrauenswürdig – demzufolge werden keine Einschränkungen für Zugriff oder Protokoll innerhalb des LAN aktiv sein. Wer im LAN ist, hat freie Bahn! An das LAN sind üblicherweise Drucker, Switches, Firewall oder W-LAN-Geräte angeschlossen. Jedes dieser Geräte ist als Außengrenze zu bewerten. Außerdem besteht über (gepatchte) Netzwerkdosen ein direkter Zugang zur Verkabelung.

Lösung: Mit allen Mitteln muss verhindert werden, dass eines der Geräte oder hereingetragene Dateien es externen Angreifern ermöglicht, eine Verbindung mit dem LAN herzustellen. Folgendes können Sie tun

- Netzwerkdosen nur für bekannte Geräte freigeben (Radius-Server)
- Firewall-Konfiguration durchgängig halten (keine "Löcher" bohren)
- USB-Ports an Druckern sperren
- W-LAN in eigener LAN-Infrastruktur betreiben (V-LAN)
- Management auf allen Switch-Geräten aktivieren

Außengrenzen Sichern

- wirksamen Virenschutz auf den Arbeitsplatz-Geräten betreiben
- wirksame SPAM-Abwehr betreiben
- USB-Ports an den Arbeitsplatz-Geräten abschalten

Society-Produkt: Mit einem Modul aus dem ‚ISM-Code‘ erhalten Sie über eine gezielte Untersuchung Ihres LAN, der Firewall und der Switches jeden möglichen Übergang benannt und können gezielte Gegenmaßnahmen einleiten.

Society-Produkt: Mit Society Ocean™ ‚Pier‘ stellen Sie sicher, dass die Sicherheit Ihrer Firewall ohne Hintertüren und „Löcher“ betrieben wird. Wirksamer Virenschutz und SPAM-Abwehr sichern Sie gegen „hereingetragene“ Angreifer.

Society-Produkt: Mit Society Ocean™ ‚Festung‘ stellen Sie sicher, dass über die Arbeitsplätze keine Schadsoftware aktiviert werden kann und der Zugriff auf Dateien stets mit dem notwendigen Misstrauen erfolgt.

4. Schaffen Sie die Gewohnheit „Anlage an E-Mail“ ab

Problem: Die E-Mail ist mit großem Anteil dafür verantwortlich, Angreifern die Möglichkeit zu geben, Schadsoftware auf Ihre Arbeitsplätze zu bringen. Mit Dateianlagen gelingt es Angreifern jeden Tag tausendfach, die Kontrolle über Arbeitsplätze (Windows) und Benutzerkonten in einem Unternehmen zu übernehmen, um unterschiedlichste kriminelle Handlungen durchzuführen. Ausführbare Programme genau wie Scripts innerhalb von Excel, Word, Powerpoint führen zu Angriffen mit dem Ziel der Spionage, Sabotage, Erpressung oder Identitätsdiebstahl.

Lösung: Schaffen Sie die Nutzung von Dateianlagen (in jeder Form) in Ihrem Unternehmen ab! Transportieren Sie keine Dateien mehr als Dateianlage in einer Mail, und nehmen auch keine Dateianlagen mehr an. Schaffen Sie zum Austausch von Dateien mit Personen eine gesonderte technische Umgebung. Mit einer sicheren Dateiablage schützen Sie auch die Informationen Ihres Unternehmens besser und verhindern unbeabsichtigten Abfluss von Informationen oder Geheimnissen an Dritte.

Außengrenzen Sichern

Society-Produkt: Mit Society Ocean™ ‚Sedimente‘ stellt Ihnen eine sichere Dateispeicher-Lösung auf der Basis von NextCloud zur Verfügung. Teilen Sie Dateien mit externen Personen, empfangen Sie Dateien auf sicherem Weg, schalten Sie Zugriffsberechtigungen auf Ordner und Dateien wirksam und umfangreich.

5. Überprüfen Sie aufgerufene Webseiten auf Angriffscodes

Problem: Angriffe erfolgen heutzutage auch über „Webseiten“. In Webseiten können Scripte und Programme von Anwender unbemerkt auf Ihre Arbeitsplätze geladen werden. Auch über die bekannten Cookies können von Angreifern Angriffe vorbereitet werden. All das geschieht vom Anwender unbemerkt auf dem Arbeitsplatz des Anwenders und führt den Angreifer zum Erfolg.

Lösung: Erlauben Sie schon auf der Firewall nicht das Öffnen bekannter gefährlicher Webseiten. Sperren Sie ggf. Seiten, weil Sie den Aufruf verhindern wollen.

Society-Produkt: Mit Society Ocean™ ‚Pier‘ stellen Sie sicher, dass „bekannte gefährliche Webseiten“ von Ihrer Firewall blockiert werden. Dadurch ist es keinem Arbeitsplatz Ihres Netzwerkes mehr möglich, gefährliche Webseiten zu öffnen.

Society-Produkt: Mit Society Ocean™ ‚Festung‘ stellen Sie sicher, dass Angriffe über eine Webseite erkannt und abgewehrt werden.

6. Awareness-Schulungen für jede Person in Ihrer IT-Anlage

Problem: bei 90% aller erfolgreichen Angriffe sind die Angriffe deshalb erfolgreich, weil die Anwender an einem PC nicht richtig reagieren. Dies liegt meistens in dem fehlenden Bewusstsein zu einer drohenden Gefahr, was dazu führt, dass Angriffe nicht als solche erkannt werden. Angriffe über Anwender sind deshalb besonders verheerend, weil die Berechtigungen des „gehackten“ Anwenders oft zu einer großen Menge an Daten und Informationen führen.

Außengrenzen Sichern

Lösung: Verbessern Sie die Gefahrenerkennung und begrenzen zusätzlich das mögliche Schadensausmaß. Sorgen Sie für eine Erweiterung des Bewusstseins der Anwender Ihrer IT.

Society-Produkt: Mit Society Ocean™ ‚ISM Code‘ schaffen Sie eine Möglichkeit zur langfristigen Ausbildung zum Thema „Awareness zur IT-Sicherheit“. Sorgen Sie mit dieser Web-basierten Ausbildung dauerhaft dafür, dass alle Anwender in Ihrem Unternehmen Kenntnisse über mögliche Angriffsformen erhalten, eine skeptische Wachsamkeit aufbauen und die Risiken und Gefahren bei der Nutzung von Internet und E-Mail kennenlernen.

(7) Berechtigungen einzelner Personen zweckmäßig eingrenzen

Problem: Wenn sich ein Angriff durchgesetzt hat, ist das Schadensausmaß entsprechend zum Umfang der Berechtigungen des betroffenen Benutzerkontos. Hier gilt die einfache Formel: kann die Person auf viele Daten zugreifen, wird der Angriff sich auf genau diese vielen Daten erstrecken.

Lösung: Sorgen Sie für eine sinnvolle Berechtigungs-Struktur auf Daten und Systeme in Ihrer IT und grenzen damit das mögliche Ausmaß an Schaden ein, weil nur dieses im Falle eines erfolgreichen Angriffes für den Angreifer nutzbar wird. Grenzen Sie also die Berechtigungen bei jedem Anwender ein, verfolgen dabei das Minimal-Prinzip, das für den Alltag der Person ausreichend ist. Wenn eine Person auch Aufgaben erledigen soll, die weitergehende Rechte benötigt, legen Sie ein zweites Anwenderkonto mit weitergehenden Rechten für diese Person an. Wichtig: Administratoren sollten niemals auf dem normalen Anwender-Account alle Rechte zur Administration erhalten.

Society-Produkt: Mit dem passenden Modul aus dem ‚ISM-Code‘ erhalten Sie über eine gezielte Untersuchung Ihrer Berechtigungs-Struktur einen Bericht und können gezielte Gegenmaßnahmen einleiten.

Society-Produkt: Mit Society Ocean™ ‚Sedimente‘ erhalten Sie eine moderne Datei—Ablage-Lösung, die Berechtigungen auf Ordner und Dateien umfangreich gestalten kann. Gestalten Sie die Dateiablage grundlegend und auf Sicherheit ausgerichtet und auf diesem Wege eine leistungsfähige File-Server-Lösung für Ihr Unternehmen.