

Sicherung der Innengrenzen Ihres Unternehmens

Autor - T. Brake

Sicherung der Innengrenzen Ihres Unternehmens

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 Personen
 - 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, Geschäftsführer oder verantwortlicher Entscheider tragen Sie die Verantwortung dafür, die Werte Ihres Unternehmens zu schützen. Diese Aufgabe steht heute nicht mehr als technisches Nebenthema am Rand, sondern gehört in dieselbe Klasse wie Wachstum, Ertrag und Führung. Sie lässt sich nicht einfach wegdelegieren. Wer Verantwortung trägt, muss auch dafür sorgen, dass Angriffe nicht nur abgewehrt, sondern in ihren Auswirkungen begrenzt werden. Genau dort beginnt die Sicherung der Innengrenzen.

Wer sind denn diese Angreifer?

Angreifer sind längst nicht mehr nur einzelne Personen. In vielen Fällen handelt es sich um organisierte Gruppen, die arbeitsteilig vorgehen und gegen Bezahlung konkrete Ziele verfolgen. Besonders gefährlich wird es dann, wenn nach einem ersten Zugriff innerhalb Ihrer IT-Struktur Bewegungsfreiheit entsteht. Der eigentliche Schaden beginnt oft nicht am Rand, sondern erst im Inneren Ihres Unternehmens.

Sicherung der Innengrenzen Ihres Unternehmens

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.

Wie muss ich mir einen Angriff im Inneren vorstellen?

Ein Angriff beginnt häufig mit einem ersten Zugang: über das Internet, über E-Mail, über einen unsicheren Fernzugriff oder über Schadsoftware auf einem Arbeitsplatz. Sobald dieser Zugang gelungen ist, versucht der Angreifer in der Regel nicht stehenzubleiben. Er sucht weitere Systeme, weitere Benutzerkonten, weitere Dateien, weitere Berechtigungen und weitere Wege in besonders wertvolle Bereiche. Aus einem kompromittierten Arbeitsplatz kann ein kompromittierter Dateibereich werden. Aus einem kompromittierten Dateibereich kann ein kompromittierter Server werden. Aus einem lokalen Vorfall kann so ein unternehmensweiter Stillstand entstehen. Diese Gefahr ist besonders groß, wenn das Innere des Unternehmens als eine einzige große Vertrauenszone betrieben wird.

Welche Folgen kann ein erfolgreicher Angriff im Inneren haben?

Die Folgen eines Angriffs hängen nicht nur davon ab, ob jemand hineingelangt, sondern vor allem davon, wie weit er danach kommt. Ohne innere Grenzen kann ein einzelner erfolgreicher Zugriff dazu führen, dass Daten kopiert, Prozesse sabotiert, Systeme verschlüsselt, Kommunikation gestört oder Identitäten missbraucht werden. Dann ist nicht mehr nur ein Gerät betroffen, sondern die Betriebsfähigkeit insgesamt. Innengrenzen sind deshalb keine technische Nebensache. Sie sind das Mittel, mit dem ein Unternehmen verhindert, dass aus einem Vorfall ein Flächenbrand wird.

Sicherung der Innengrenzen Ihres Unternehmens

Sicherung der Innengrenzen Ihres Unternehmens

Die Innengrenzen Ihres Unternehmens beginnen dort, wo nach einem ersten Zugriff nicht mehr alles mit allem verbunden sein darf. Während die Außengrenzen den Einstieg erschweren sollen, sorgen Innengrenzen dafür, dass sich ein Angreifer nach einem gelungenen Einstieg nicht ungehindert ausbreiten kann. Es geht darum, interne Bereiche so zu gliedern, dass Rechte, Daten, Systeme und Kommunikation voneinander abgegrenzt werden und Übergänge nur dort möglich sind, wo sie geschäftlich wirklich gebraucht werden.

Der Universal-Schutz

Im Inneren Ihres Unternehmens besteht Schutz nicht darin, alles zu erlauben und auf gutes Verhalten zu hoffen. Die entscheidende Hauptregel lautet: Vertrauen muss begrenzt, gegliedert und kontrolliert werden. Was nicht jeder sehen, erreichen, starten oder verändern muss, darf auch nicht allgemein offenstehen.

Dabei ist zu beachten, dass ...

Innengrenzen nicht nur aus Technik bestehen. Sie entstehen durch Netztrennung, durch Berechtigungen, durch die Art des Arbeitsplatzbetriebs, durch den Ort der Datenablage, durch den Betrieb von Kommunikationssystemen und durch die Frage, wie professionell die zentralen Dienste Ihres Unternehmens geführt werden. Ein Unternehmen besitzt also nicht nur Räume und Netzwerke, sondern auch innere Sicherheitszonen: Dateibereiche, Benutzerrollen, Serverdienste, E-Mail-Systeme, Arbeitsplätze, Backups und betriebliche Kernsysteme. Werden diese Zonen sauber getrennt und kontrolliert betrieben, dann verliert ein Angreifer Bewegungsfreiheit.

Sicherung der Innengrenzen Ihres Unternehmens

Folgende 7 Aktionen begrenzen die Ausbreitung eines Angriffs

1. Gliedern Sie Ihr internes Netzwerk in klar getrennte Sicherheitszonen

Problem: In vielen Unternehmen ist das interne Netzwerk historisch gewachsen. Arbeitsplätze, Drucker, Server, W-LAN, Telefonie, Fernzugänge und Verwaltungszugänge liegen logisch zu nah beieinander. Wer an einer Stelle Fuß fasst, findet dadurch oft sofort weitere Wege.

Lösung: Teilen Sie Ihr internes Netzwerk in sinnvolle Zonen. Trennen Sie mindestens Arbeitsplätze, Serverdienste, Druck- und Infrastruktursysteme, W-LAN, Fernzugriffe und administrative Zugänge sauber voneinander. Definieren Sie nur die Übergänge, die im Alltag wirklich gebraucht werden, und überwachen Sie diese Übergänge bewusst.

Tipp: Beginnen Sie nicht mit Technik, sondern mit einer einfachen Landkarte. Zeichnen Sie auf, welche Systeme intern miteinander sprechen dürfen und welche besser gar keinen direkten Kontakt haben sollten.

Society-Produkt: Mit **Society Ocean™ „Pier“** steht eine zentral betriebene Firewall-Absicherung des LANs zur Verfügung, inklusive Intrusion Prevention, Gateway Antivirus, Application Control, Network Discovery, zentraler Verwaltung, Protokollierung sowie VPN mit 2-Faktor-Authentifizierung. Diese Bausteine helfen dabei, interne Übergänge kontrolliert und nicht zufällig zu betreiben.

Sicherung der Innengrenzen Ihres Unternehmens

2. Stellen Sie Arbeitsplätze standardisiert und zentral bereit

Problem: Einzelne lokal gewachsene PCs mit unterschiedlichem Zustand, unterschiedlicher Softwarebasis und unterschiedlicher Pflege machen das Innere eines Unternehmens unübersichtlich. Jeder abweichende Arbeitsplatz wird zu einer eigenen Sonderzone mit schwer kalkulierbarem Risiko.

Lösung: Schaffen Sie ein einheitliches Arbeitsplatzmodell. Trennen Sie möglichst klar zwischen Endgerät und eigentlichem Arbeitsumfeld. Je standardisierter Arbeitsplätze bereitgestellt und verwaltet werden, desto leichter lassen sich Rechte, Softwarestände und Reaktionen auf Vorfälle steuern.

Tipp: Besonders bei Onboarding, Homeoffice oder wechselnden Leistungsanforderungen zeigt sich schnell, wie wertvoll zentral bereitgestellte Arbeitsplätze sind. Sie reduzieren Improvisation und schaffen Ordnung.

Society-Produkt: *Society Ocean™ „Population“* stellt virtuelle Windows-Desktops inklusive Unternehmensanwendungen zentral bereit. Der Zugriff ist von verschiedenen Geräten möglich, Arbeitsplätze lassen sich schnell bereitstellen, zentral verwalten und bei Bedarf in CPU und RAM anpassen. Daraus ergibt sich eine deutlich besser steuerbare Arbeitsplatzlandschaft.

Sicherung der Innengrenzen Ihres Unternehmens

3. Verlagern Sie Dateien und Zusammenarbeit in eine kontrollierte Plattform

Problem: Dateien, die auf lokalen PCs, in E-Mail-Anhängen, auf verstreuten Laufwerken oder in schlecht geordneten Freigaben liegen, durchbrechen jede innere Ordnung. Versionen geraten durcheinander, Berechtigungen werden unsauber, und Informationen verlassen das Unternehmen schneller, als man es bemerkt.

Lösung: Führen Sie Dateien, Freigaben und Zusammenarbeit auf einer zentralen Plattform zusammen. Dateien sollten nicht über unkontrollierte Wege verteilt, sondern gezielt bereitgestellt, synchronisiert und freigegeben werden. Das schafft Übersicht und senkt das Risiko, dass ein Vorfall sich über Dateichaos weiter ausbreitet.

Tipp: Verbinden Sie diesen Schritt mit einer klaren Regel: Geschäftlich relevante Dateien gehören in definierte Bereiche und nicht in Postfächer oder lokale Sonderablagen.

Society-Produkt: *Society Ocean™ „Sedimente“* stellt eine zentrale Datei-Plattform auf Basis von Nextcloud bereit. Sie ermöglicht sicheren ortsunabhängigen Zugriff, Team-Zusammenarbeit, mobile Nutzung, Teilen ohne E-Mail-Anhänge sowie umfangreiche Berechtigungen auf Dateien und Ordnern. Zusätzlich werden regelmäßige Updates, Verschlüsselung sowie Schutzmechanismen gegen Brute-Force- und Ransomware-Angriffe beschrieben.

Sicherung der Innengrenzen Ihres Unternehmens

4. Grenzen Sie Berechtigungen konsequent nach Zweck und Rolle ein

Problem: Das Schadensausmaß eines erfolgreichen Angriffs wächst mit den Rechten des betroffenen Kontos. Wer auf viele Daten zugreifen darf, eröffnet genau dort auch dem Angreifer Möglichkeiten. Besonders kritisch wird es, wenn erhöhte Rechte im Alltag dauerhaft mitgeführt werden.

Lösung: Verfolgen Sie konsequent das Minimal-Prinzip. Jeder Benutzer erhält nur die Rechte, die für die tägliche Arbeit notwendig sind. Weitergehende Rechte gehören in gesonderte Konten oder klar definierte Sonderrollen. Prüfen Sie Berechtigungen regelmäßig und entfernen Sie gewachsene Altlasten.

Tipp: Dort, wo Verantwortlichkeiten unklar sind, entstehen fast immer zu breite Berechtigungen. Rollen müssen fachlich begründet und technisch sauber umgesetzt sein.

Society-Produkt: Für Datei- und Ordnererebenen bietet **Society Ocean™ „Sedimente“** die Möglichkeit, Berechtigungen umfangreich zu gestalten und damit innere Grenzen in der Zusammenarbeit sauber abzubilden. So lässt sich das Minimal-Prinzip nicht nur beschließen, sondern praktisch umsetzen.

Sicherung der Innengrenzen Ihres Unternehmens

5. Behandeln Sie E-Mail, Groupware und Telefonie als geschützten inneren Kern

Problem: Kommunikation ist nicht nur Hilfsmittel, sondern ein zentraler Betriebsprozess. Wenn Mail, Groupware oder Telefonie improvisiert betrieben werden, hängen Verfügbarkeit, Sicherheit und Nachvollziehbarkeit oft an Einzelwissen, alten Konfigurationen oder fehlender Dokumentation.

Lösung: Führen Sie Kommunikationsdienste strukturiert und nachvollziehbar. Mailserver, Groupware, Archivierung und Telefonie gehören in einen geregelten Betrieb mit Updates, Monitoring, Datensicherung und klaren Wiederherstellungswegen.

Tip: Kommunikation muss auch dann funktionieren oder zumindest sauber wiederherstellbar sein, wenn ein einzelnes System, eine Person oder ein Standort ausfällt.

Society-Produkt: *Society Ocean™ „Welle“* beschreibt die Migration und den Managed Betrieb von Mailserver und Groupware auf Basis von grommunio, inklusive 24/7 Monitoring, Updateservice, Datensicherung und Security.

Society Ocean™ „Schlick“ ergänzt dies um eine automatische Archivierung sämtlicher ein- und ausgehender E-Mails sowie die Wiederherstellbarkeit gelöschter Nachrichten. Für die Telefonie stellt ***Society Ocean™ „Blubbern“*** eine UC-Telefonanlage aus dem Datacenter mit Updates, Monitoring, Entstörung, Backup und flexibler Skalierung bereit.

Sicherung der Innengrenzen Ihres Unternehmens

6. Sorgen Sie dafür, dass ein Vorfall nicht zum endgültigen Datenverlust wird

Problem: Selbst gute Innengrenzen verhindern nicht jeden Schaden. Dateien können gelöscht, Systeme beschädigt oder Datenbestände verschlüsselt werden. Wenn dann keine belastbare Wiederherstellung möglich ist, wird aus einem Sicherheitsvorfall sehr schnell ein existenzielles Betriebsproblem.

Lösung: Trennen Sie Produktivbetrieb und Wiederherstellung konsequent. Ein Backup muss an einem anderen Ort liegen, regelmäßig kontrolliert werden und im Ernstfall tatsächlich zur Rücksicherung taugen. Nur so wird aus einer Störung ein beherrschbarer Vorfall statt eines Totalverlusts.

Tipp: Sichern Sie nicht nur Server. Prüfen Sie auch Arbeitsplätze, Microsoft-365-Daten, Datenbanken und geschäftskritische Anwendungen.

Society-Produkt: *Society Ocean™ „Muschel“* beschreibt eine Offsite-Datensicherung im Rechenzentrum für physische und virtuelle Server, Workstations, Microsoft-365-Daten, Datenbanken und Anwendungen. Der Backup-Status ist schnell erkennbar; Wiederherstellung und planbare Kosten stehen im Mittelpunkt. Damit entsteht ein wirksamer Rückzugsraum für den Fall, dass innere Bereiche bereits beschädigt wurden.

Sicherung der Innengrenzen Ihres Unternehmens

7. Bündeln Sie kritische interne Dienste in einer professionellen Betriebsumgebung

Problem: Ein eigener Serverraum, verschobene Wartung, alternde Hardware und schwer planbare Kapazitäten führen dazu, dass zentrale Dienste zwar vorhanden, aber nicht belastbar genug betrieben werden. Gerade dort entstehen Schwächen, die ein Angreifer nach einem ersten Zugriff ausnutzen kann.

Lösung: Prüfen Sie, welche Kernsysteme in einer professionellen Umgebung besser aufgehoben sind als im gewachsenen Eigenbetrieb. Wo Betrieb, Sicherheit, Wartung und Skalierung sauber organisiert sind, verlieren Störungen und Angriffe an Wirkung.

Tipp: Nicht jede interne Leistung muss lokal betrieben werden. Entscheidend ist, ob der Betriebsort zur geschäftlichen Bedeutung des Systems passt.

Society-Produkt: *Society Ocean™ „Habitat“* wird als IT-Infrastruktur-as-a-Service beschrieben und dient als Alternative zum eigenen Serverraum. Es umfasst zentrale IT-Dienste wie E-Mail, Datenbanken, VoIP-Telefonie und Anwendungen, kombiniert mit regelmäßiger Wartung, Sicherheitsstandards, Skalierbarkeit und schneller Implementierung. Für Unternehmen, die ihre Kernsysteme stabiler und kontrollierter betreiben wollen, ist das ein naheliegender Baustein.

Sicherung der Innengrenzen Ihres Unternehmens

Kontaktieren Sie uns noch heute für ein kostenloses Erstgespräch!

Kontaktaufnahme über

- Kontaktformular: **society.de**
- Telefon: +49 221 337759-0
- E-Mail: team@society.de

Unsere Gesprächszeiten

Montag bis Donnerstag

- 09:00 - 13:00 Uhr
- 14:00 - 18:00 Uhr

Freitag

- 09:00 - 11:30
- 14:00 - 18:00

