

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

Autor - T. Brake

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

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, als Geschäftsführer und auch als Entscheider haben Sie die Verantwortung, die Werte Ihres Unternehmens zu schützen. Diese Aufgabe nimmt heute den gleichen Stellenwert ein wie Wachstum, Ertrag und Management. Schutz und Abwehr sind keine technische Nebensache. Sie gehören zur Führungsaufgabe. Gerade deshalb darf die Frage nach Schwachstellen im Unternehmens-Netzwerk nicht dem Zufall überlassen werden. Wer die eigenen Schwachpunkte nicht kennt, überlässt dieses Wissen im schlimmsten Fall dem Angreifer.

Wer sind denn diese Angreifer?

Angreifer sind heutzutage längst keine Einzelpersonen mehr, sondern häufig bandenartig tätige Gruppen, die regelrecht beauftragt werden, bestimmte Ziele zu erreichen. Diese Ziele reichen von Sabotage über Datendiebstahl bis hin zur Erpressung. Ein erfolgreicher Angriff beginnt oft nicht mit Gewalt, sondern mit einer unbemerkten Schwachstelle: einer falsch konfigurierten Firewall-Regel, einem offenen Übergang im LAN, einem zu weit berechtigten Benutzerkonto oder einem unscheinbaren Gerät, das nie in eine Prüfung einbezogen wurde.

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

Welche Unternehmen werden denn angegriffen?

Es spielt keine wesentliche Rolle, welche Größe Ihr Unternehmen hat. Solange es über Daten, Kommunikation, Betriebsfähigkeit, Geld oder leistungsfähige Mitarbeiter verfügt, lohnt sich ein Angriff. Jedes Unternehmen besitzt digitale Übergänge und technische Abhängigkeiten. Genau dort entstehen Schwachstellen. Je weniger diese Übergänge bekannt und kontrolliert sind, desto größer ist das Risiko, dass ein Angreifer sie vor Ihnen entdeckt.

Wie muss ich mir Schwachstellen in meinem Unternehmens-Netzwerk vorstellen?

Schwachstellen entstehen nicht nur an einem einzelnen Gerät. Sie entstehen in Übergängen, Berechtigungen, Konfigurationen und Gewohnheiten. Eine Schwachstelle kann in der Firewall liegen, im W-LAN, in einer Netzwerkdose, in einem Switch, in einem veralteten Arbeitsplatz, in einem VPN-Zugang oder in einer Anwendung, die unbemerkt von außen erreichbar ist. Oft ist nicht ein einzelner Fehler das Problem, sondern die Kombination vieler kleiner Nachlässigkeiten. Genau diese Kombinationen machen professionelle Prüfungen so wertvoll.

Warum werden Schwachstellen oft zu spät erkannt?

Weil gewachsene IT-Strukturen auf den ersten Blick oft funktionieren. Das Netzwerk läuft, die Mitarbeiter arbeiten, die Geräte antworten. Doch Betriebsfähigkeit ist kein Beweis für Sicherheit. Häufig wurde nie sauber dokumentiert, welche Systeme vorhanden sind, welche Übergänge existieren, welche Regeln gelten und welche Rechte wirklich gebraucht werden. In einem solchen Zustand bleiben Schwachstellen oft lange unentdeckt - bis ein Störfall, ein Angriff oder eine Fehlbedienung sie sichtbar macht.

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

Welche Folgen kann eine unbekannte Schwachstelle haben?

Bedenken Sie, dass ein Angriff nicht nur einzelne Geräte betreffen muss. Schon eine übersehene Schwachstelle kann dazu führen, dass Angreifer in Ihr Netzwerk eindringen, sich weiterbewegen, Daten kopieren, Kommunikation stören, Arbeitsplätze übernehmen oder Betriebsabläufe unterbrechen. Im schlimmsten Fall wird Ihr Unternehmen tagelang oder sogar über Wochen in seiner Arbeitsfähigkeit massiv eingeschränkt. Wer Schwachstellen kennt, kann gegensteuern. Wer sie nicht kennt, trägt das Risiko blind.

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

Jedes Unternehmens-Netzwerk besitzt technische und organisatorische Übergänge, an denen Risiken entstehen. Die professionelle Überprüfung auf Schwachstellen verfolgt daher ein klares Ziel: vorhandene Angriffsflächen sichtbar machen, deren Bedeutung bewerten und konkrete Gegenmaßnahmen ableiten, bevor ein Angreifer diese Schwachstellen ausnutzt.

Der Universal-Schutz

Er besteht nicht darin, auf Glück zu vertrauen oder einzelne Geräte irgendwie sicher zu halten. Die wesentliche Hauptregel lautet: Nur was Sie kennen, bewerten und kontrollieren, können Sie wirksam schützen. Eine Schwachstellenprüfung schafft deshalb zuerst Klarheit - und genau diese Klarheit ist die Voraussetzung für Resilienz.

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

Dabei ist zu beachten, dass ...

... die Überprüfung eines Unternehmens-Netzwerkes eine komplexe Angelegenheit ist. Es gibt physische Übergänge, logische Übergänge, technische Geräte, Benutzerkonten, Anwendungen, externe Anbindungen, mobile Arbeitsweisen und historisch gewachsene Sonderlösungen. Nicht jede Auffälligkeit ist automatisch kritisch. Nicht jede vermeintlich sichere Umgebung ist tatsächlich belastbar. Hier hilft nur eine systematische Untersuchung durch einen Fachmann, der vorhandene Risiken erkennt, einordnet und in einen sinnvollen Maßnahmenkatalog überführt.

Es ist wichtig zu verstehen, dass ...

... ein Unternehmens-Netzwerk aus weit mehr als ein paar Switches und Kabeln besteht. Zum Netzwerk gehören unter anderem Firewall, Internet-Anbindung, VPN-Zugänge, W-LAN, Arbeitsplatz-Geräte, Drucker, Server, zentrale Dienste, Dateiaustauschwege und die Struktur der Berechtigungen. Genau genommen ist jede Stelle, an der Daten fließen, Rechte vergeben werden oder Systeme miteinander sprechen, ein möglicher Übergang - und damit ein möglicher Schwachpunkt

Man muss sich klar machen, dass ...

...es bei einer Schwachstellenprüfung nicht um Theorie geht, sondern um konkrete Gefahren: Sabotage, Spionage, Datendiebstahl, missbrauchte Identitäten, Schadsoftware, unerwünschte Fernzugriffe und Betriebsunterbrechungen. Ziel der Prüfung ist deshalb nicht bloß ein technischer Bericht, sondern die Grundlage für konkrete Entscheidungen.

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

Folgende 7 Aktionen helfen dabei, Schwachstellen im Netzwerk sichtbar zu machen!

In den folgenden 7 Schritten erreichen Sie es, Ihr Unternehmens-Netzwerk strukturiert zu prüfen. Auf diese Weise erkennen Sie offene Übergänge, bewerten Risiken fachlich und schaffen eine belastbare Grundlage für wirksame Gegenmaßnahmen.

1. Erstellen Sie eine vollständige Landkarte Ihres Netzwerkes

Problem: In vielen Unternehmen existiert keine vollständige Übersicht über alle Geräte, Übergänge, Dienste und Netzsegmente. Dadurch bleiben kritische Schwachpunkte unsichtbar

Lösung: Erfassen Sie systematisch, welche Geräte, Verbindungen, Dienste, Standorte, W-LAN-Strukturen, VPN-Zugänge und administrativen Übergänge vorhanden sind. Erst auf dieser Grundlage lässt sich fachlich bewerten, wo Risiken bestehen.

Tipp: Zeichnen Sie Ihr Netzwerk nicht nur technisch, sondern auch funktional auf. Wichtig ist nicht nur, was vorhanden ist, sondern auch, wozu es dient und mit wem es sprechen darf.

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.

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

2. Prüfen Sie Firewall, Internet-Zugänge und Fernzugriffe

Problem: Internet-Anbindung, Firewall-Regeln und VPN-Zugänge gehören zu den bevorzugten Ansatzpunkten eines Angreifers. Falsch gesetzte Regeln, veraltete Signaturen oder unklare Fernzugriffe vergrößern die Angriffsfläche.

Lösung: Prüfen Sie sämtliche Regeln, Freigaben, Weiterleitungen und Zugriffswege auf Notwendigkeit, Aktualität und technische Sauberkeit. Besonders Fernzugriffe und standortübergreifende Verbindungen müssen konsequent bewertet werden.

Tipp: Fragen Sie bei jeder Regel und bei jedem Übergang: Wird das wirklich noch gebraucht? Wenn die Antwort nicht eindeutig ist, gehört der Punkt auf den Prüfstand.

Society-Produkt: **Society Ocean™ „Pier“** beschreibt eine Managed Firewall mit Intrusion Prevention, Gateway Antivirus, zentraler Verwaltung, 24/7 Monitoring, Sicherheitsupdates, Application Control, Network Discovery und VPN mit 2-Faktor-Authentifizierung. Genau diese Bausteine sind für die saubere Überprüfung und Absicherung solcher Übergänge relevant.

3. Untersuchen Sie LAN, Switches, W-LAN und Netzwerkdosen gezielt

Problem: Wer sich im lokalen Netzwerk bewegt, trifft in vielen Umgebungen auf zu viel Vertrauen. Ungeschützte Netzwerkdosen, unklare Switch-Konfigurationen, schlecht getrennte W-LAN-Strukturen oder offen gelassene Management-Zugänge eröffnen unnötige Wege.

Lösung: Untersuchen Sie Ihr LAN gezielt auf Übergänge, die Angreifern oder ungewollten Geräten Bewegungsfreiheit verschaffen können. Dazu gehören Switches, Drucker, W-LAN-Geräte, Netzwerkdosen und Management-Zugänge.

Tipp: Gerade lokale Übergänge werden oft nicht regelmäßig geprüft, weil sie im Haus liegen. Genau deshalb lohnt sich hier ein besonders nüchterner Blick.

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

Society Produkt: Das Referenz-Whitepaper nennt ausdrücklich die gezielte Untersuchung von LAN, Firewall und Switches, um mögliche Übergänge zu benennen und Gegenmaßnahmen einzuleiten. Ergänzend nennt „**Pier**“ Network Discovery sowie die zentrale Absicherung des LANs.

4. Beziehen Sie Arbeitsplatz-Geräte konsequent in die Prüfung ein

Problem: Arbeitsplatz-Geräte werden häufig nur als Arbeitsmittel betrachtet, tatsächlich sind sie aber ein besonders häufiger Eintritts- und Verbreitungsweg für Angriffe. Veralterte Systeme, Schadsoftware, unsichere Browser-Nutzung oder lokale Sonderlösungen erhöhen das Risiko erheblich.

Lösung: Beziehen Sie Endgeräte, deren Schutzstatus, deren Softwarestand sowie deren Einbindung ins Netzwerk konsequent in die Analyse ein. Prüfen Sie auch, ob Arbeitsplätze technisch zu unterschiedlich und dadurch schwer kontrollierbar geworden sind.

Tipp: Je stärker Arbeitsplätze vereinheitlicht und zentral betrieben werden, desto leichter lassen sich Auffälligkeiten erkennen und Schwachpunkte dauerhaft reduzieren.

Society Produkt: **Society Ocean™ „Population“** stellt virtuelle Windows-Arbeitsplätze zentral bereit und unterstützt damit eine standardisierte, zentral verwaltbare Arbeitsplatzumgebung. Ergänzend trägt „**Pier**“ mit Gateway-Schutz und laufenden Sicherheitsupdates zur Reduzierung eingetragener Risiken bei.

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

5. Prüfen Sie Berechtigungen und administrative Sonderwege

Problem: Schwachstellen entstehen nicht nur in Technik, sondern auch in zu weit gefassten Rechten. Unnötige Berechtigungen, gemeinsam genutzte Konten oder dauerhaft vergebene administrative Rechte vergrößern das Schadensausmaß erheblich.

Lösung: Untersuchen Sie die Berechtigungs-Struktur auf Daten, Systeme, Freigaben und Administrationszugänge. Verfolgen Sie konsequent das Minimal-Prinzip und trennen Sie Alltagsarbeit von erhöhten Rechten.

Tipp: Besonders kritisch sind Altlasten: ehemalige Zuständigkeiten, alte Freigaben, vergessene Gruppen oder Admin-Rechte, die vorsichtshalber nie entfernt wurden.

Society-Produkt: Das Referenz-Whitepaper beschreibt die gezielte Untersuchung der Berechtigungs-Struktur als Grundlage für Gegenmaßnahmen. Für Datei- und Ordnerrechte bietet **Society Ocean™ „Sedimente“** eine moderne Datei-Ablage-Lösung mit umfangreich gestaltbaren Berechtigungen.

6. Bewerten Sie auch Wiederherstellbarkeit und Ausfallfolgen

Problem: Eine Schwachstelle ist nicht nur dort kritisch, wo ein Angriff gelingt, sondern auch dort, wo sich ein Schaden nicht sauber begrenzen oder beheben lässt. Fehlen Backups oder Wiederherstellungswege, wird aus einer Schwachstelle schnell ein Betriebsproblem.

Lösung: Prüfen Sie bei kritischen Systemen immer mit, ob Daten, Konfigurationen und Dienste im Schadensfall zuverlässig wiederhergestellt werden können. Die Analyse von Schwachstellen muss also auch die Frage nach der Rückfallebene einschließen.

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

Tipp: Fragen Sie nicht nur, ob es ein Backup gibt. Fragen Sie, was gesichert wird, wo es liegt und ob eine Rücksicherung im Ernstfall realistisch funktioniert.

Society-Produkt: *Society Ocean™ „Muschel“* beschreibt eine Offsite-Datensicherung im Rechenzentrum für Server, Workstations, Microsoft-365-Daten, Datenbanken und Anwendungen. Damit lässt sich die Folgenbewertung technischer Schwachstellen deutlich belastbarer vornehmen.

7. Wiederholen Sie die Überprüfung regelmäßig und leiten Sie Maßnahmen ab

Problem: Eine einmalige Prüfung reicht nicht aus. Netzwerke verändern sich, Geräte kommen hinzu, Regeln wachsen, Zuständigkeiten wechseln und neue Risiken entstehen. Ohne Wiederholung veraltet jede Bestandsaufnahme.

Lösung: Führen Sie Schwachstellenprüfungen in wiederkehrenden Abständen durch, dokumentieren Sie die Ergebnisse sauber und priorisieren Sie Maßnahmen nach Risiko, geschäftlicher Bedeutung und Umsetzbarkeit.

Tipp: Nicht jede Schwachstelle muss sofort beseitigt werden. Aber jede relevante Schwachstelle muss bekannt, bewertet und mit einer Entscheidung versehen sein.

Society-Produkt: Der „ISM-Code“ ist als modulare Grundlage für gezielte Untersuchungen und daraus abgeleitete Gegenmaßnahmen beschrieben. Genau dadurch wird aus einer Prüfung ein handhabbarer Maßnahmenkatalog statt einer bloßen Liste technischer Auffälligkeiten.

Überprüfung Ihres Unternehmens-Netzwerkes auf Schwachstellen

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

