

IT Sicherheit • Risiken kennen und Gefahren abwehren

Überblick

Mit diesem Dokument möchte ich Ihnen einige Gedankenanstöße geben, warum Sie sich mit der IT Sicherheit in Ihrem Unternehmen beschäftigen sollten. Ich möchte dabei aufzeigen, dass es in der Regel weniger die technischen Defizite sind, die zum Problem werden, sondern viel mehr schlecht abgestimmte oder fehlende Prozesse sowie eine mangelhafte Sensibilisierung der Mitarbeiter.

Ein schlüssiges IT Sicherheitskonzept schützt Ihre Systeme, Informationen und Daten, die in der heutigen Zeit eine wesentliche Grundlage Ihrer Geschäftsprozesse sind. Machen Sie sich bewusst, wie sehr Ihr wirtschaftlicher Erfolg von der Verfügbarkeit und Integrität der Informationstechnologie abhängig ist!

In der aktuellen Situation ist es unerlässlich, Ihren Kunden und Ihren Finanzgebern gegenüber aufzuzeigen, dass die IT Sicherheit - *als wesentlicher Bestandteil des unternehmerischen Risikomanagements* - in Ihrem Hause die notwendige Beachtung findet.

Schließen Sie technische Lücken, fahrlässiges Handeln und naives Unterlassen aus, um Ihr Unternehmen nicht zu gefährden.

Die Risiken für Ihr Geschäft entstehen z.B. durch

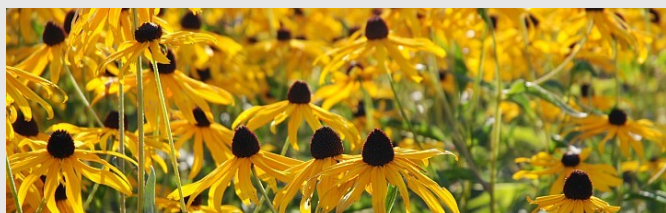
- Missbrauch
- Sabotage und Spionage
- Datenverlust
- Produktionsunterbrechungen / -ausfall

Diese Risiken erscheinen Ihnen möglicherweise als vernachlässigbar. Bedenken Sie jedoch, was sind die Folgen wenn ...

- Ihre Personalabrechnungsdaten frei im Unternehmen kursieren?
- Ihr Internetzugang, von den Nachbarn für illegale Dinge missbraucht wird?
- Kundenauftragsdaten für immer im Nichts verschwinden, weil keine Sicherung mehr auffindbar ist?
- Ihre Buchhaltung eine Woche nicht arbeiten kann?
- Ihre Kundendatei im Internet unter Spammern gehandelt wird?
- Fremde im Namen Ihrer Firma auftreten.

Gegen all diese Gefährdungspotentiale wird es Ihnen kaum gelingen, eine 100%igen Schutz zu erlangen. Sie können jedoch mit kleinen Schritten bereits eine große Wirkung erzielen.

Es werden für die IT Sicherheit oft enorme Investitionen in einem Teilbereich getätigt, jedoch auch die direkt angrenzende Hintertür weit offen gelassen. Die Gesamtbetrachtung der IT Infrastruktur, verbunden mit einer klaren Definition Ihrer Anforderungen, ermöglicht einen effizienten Weg beim Thema IT Sicherheit.



Gefahren und Risiken • Wer greift uns warum an?

- Externe undefinierte Angriffe
 - ↳ Jugendliche ohne konkrete Absichten erstellen Schadcode und greifen als Zeitvertreib ihre Systeme an.
 - ↳ Betreiber von Spam und Denial of Service (DoS) Infrastrukturen versuchen Ihre Systeme zu entern und für ihre Zwecke zu nutzen.
- Externe gezielte Angriffe
 - ↳ Ausspähen von Daten beim elektronischen Zahlungsverkehr
 - ↳ Die Konkurrenz versucht mittels Wirtschaftsspionage Informationen über Forschungsergebnisse, Produkte oder Preiskalkulationen zu erlangen.
 - ↳ Geheimdienste handeln im Sinne einer nationalen Wirtschaftspolitik.
- Interne Angriffe (Die Mehrheit aller Angriffe!)
 - ↳ Gezielte Sabotage und Diebstahl durch Mitarbeiter.
 - ↳ Unzufriedene oder gekündigte Mitarbeiter versuchen "verbrannte Erde" zu hinterlassen.
 - ↳ Mobbing und andere Interne Auseinandersetzungen.

Nachlässigkeit und ein fehlendes IT Konzept

- Die IT Infrastruktur stellt sich manchmal leider als Stückwerk dar.
- Veraltete Soft- und Hardware ohne Support durch den Hersteller.
- Bypass-Lösungen verbleiben oft als Dauerzustand. Keine wirklichen Lösungen werden erarbeitet und dokumentiert.

Der PC als Alleskönner

- Eine beliebige Mengen an Software, teils unbekannter Herkunft, wird installiert. Schlimmstenfalls durch die Mitarbeiter selbst.
- Die Standardsoftware soll genauso laufen wie spezielle, selbst programmierte Maschinensteuerungen.

Halbfertige Lösungen, fehlende Betriebs- und Supportkonzepte

- Ca. 70 % aller IT Projekte erreichen ihr Ziel nicht im vollem Umfang, sofern es ein klar formuliertes Ziel überhaupt gab. Fast 30% der Projekte erreichen überhaupt kein Ergebnis.
- Die Planung, die Implementierung und der Betrieb werden nicht voneinander abgegrenzt. Die Ziele bleiben während des Projektes variabel und eine formale Abnahme findet nicht statt.

Technologie

- Neue Technologien werden ohne Sicherheitskonzept betrieben, oder Sicherheitsmechanismen werden nicht getestet.
- Technologische Spielwiesen deren betrieblicher Nutzen nur schwer aufgezeigt werden kann, stellen ein unnötiges Risiko dar.

IT Sicherheit • Risiken kennen und Gefahren abwehren

Abhängigkeit

- Lösungen hängen zu oft an einzelnen Personen. Wissensmonopole werden aufgebaut, um unersetzlich zu sein.
- Fehlende Dokumentationen erzeugen Abhängigkeit, da den Kollegen die Möglichkeit fehlt, sich in die Materie einzuarbeiten.
- Behelfslösungen werden über die Zeit zu unternehmenskritischen Applikationen.

Welche Risiken hat das Alles für ihr Geschäft?

- Unkalkulierbare Kosten
- Verlust von Kunden und Mandanten
- Haftung der Geschäftsführung bei Fahrlässigkeit und Unterlassen
- Imageverlust in der Öffentlichkeit
- Risiken in der Archivierungspflicht (z.B. gegenüber Finanzamt)

Regeln und Vorgaben

Durch unser Verhalten beeinflussen wir die Wirkungsweise der Sicherheitsmaßnahmen. Aus Bequemlichkeit umgehen wir gerne Regeln und erzeugen unnötige Risiken.

Was können wir regeln?

- Nutzungsvereinbarung für das IT Inventar, Internet und das Mailsystem
- Die private Nutzung der IT Infrastruktur
- Die Rechte und Pflichten unserer Lieferanten

Was können wir nicht regeln?

- Den Inhalt der Mails von Mitarbeitern
- Das Verhalten Dritter (Kunden, Nachbarn, Behörden...)

Regel Nr. 1: Verständliche Regeln

Technisch überfrachtete Anleitungen bringen nichts. Wenn deren Sinn nicht ersichtlich ist und auch nicht erläutert wird, werden die Regeln ignoriert.

Gewohnheitsrecht

Wenn Regelungen nicht tatsächlich durchgesetzt werden sind sie arbeitsrechtlich nur kaum verwertbar. Besonders schwierig ist dies bei Fragen zur Haftung zu sehen! Die Kenntnis der Regelungen sollte durch die Mitarbeiter schriftlich dokumentiert werden.

Da hilft keine Technik: „Social Engineering“

Mittels "sozialer Kontakte" und deren geschickter Ausnutzung lassen sich Sicherheitsmaßnahmen umgehen. Dieses Vorgehen ist gegenüber konventionellen Angriffen einfacher, billiger und oft auch deutlich schneller und so gut wie immer erfolgreich. Leider ist keine Abwehr durch Vorschriften oder technische Lösungen möglich, allein durch Training und Sensibilisierung der Mitarbeiter wird "Social Engineering" weniger erfolgreich.

Vorkehrungen und Maßnahmen

Man kann einige Standards benennen, die aus Sicht der IT-Sicherheit unerlässlich sind. Dazu gehören unter anderem:

- Arbeiten unter „eigenem Namen“, d.h. alle Mitarbeiter loggen sich mit einem eigenen Account ein.
- Die Klassifizierung von Informationen. Sensible Daten (Geschäftsstrategie, Kalkulationen, Personaldaten) müssen als vertraulich eingestuft und entsprechen geschützt werden.
- „Need to know“-Prinzip: Der Zugang zu Daten ist restriktiv. Jeder sieht nur das, was er für seine Arbeit benötigt.

Technik muss natürlich auch sein

Dies ist nur eine Aufzählung einiger absolut notwendiger Mindestanforderungen.

Netzwerk- und physische Sicherheit

- Ihr Netzwerk sollte mit den Standards an Sicherheitsmechanismen ausgestattet sein. Niemand darf sich mit dem Netz ohne Ihr Wissen verbinden, weder drahtlos noch per Kabel. Ebenso dürfen Ihre IT Endgeräte nicht ungesichert in Fremdnetzwerken betrieben werden.
- Ihre Server- und Netzwerkinfrastruktur muß verschlossen werden. Nur die Administratoren dürfen Zugriff auf die Geräte haben.

Viren und Firewalls

- Eine Sicherung ALLER Endgeräte und Server mit einer aktuellen Virenschutzsoftware ist selbstverständlich.
- Ihr Netzwerk ist nach außen durch mindestens eine Firewall zu sichern. Sorgen Sie dafür, dass keine alternativen Wege zu Fremdnetzen (insbesondere zum Internet!) zugelassen und möglich sind.
- Nutzen Sie für den Austausch mit Kunden und Lieferanten grundsätzlich gesicherte Verbindungswege.

Systemwartung

- Stellen Sie sicher, dass alle Systeme mit den notwendigen Sicherheitsupdates versorgt werden.
- Vermeiden Sie den Betrieb von Systemen, für die durch den Hersteller kein Support mehr angeboten wird.

Administrator-Rechte

- Behandeln Sie Administratorrechte extrem restriktiv. Mit Hilfe dieser Rechte können so gut wie alle Sicherheitsmechanismen außer Kraft gesetzt werden.

Verschlüsselung

- Verschlüsseln Sie vertrauliche Mails grundsätzlich.
- Verschlüsselung der Daten auf Fileservern und insbesondere Notebooks, um Zugriff durch Unberechtigte zu verhindern.

Besprechen Sie dieses Thema mit mir und lassen Sie uns gemeinsam herausfinden, mit welchen Massnahmen Sie Ihr Unternehmen ein gutes Stück sicherer machen können.