MARKEL®

Markel Pro Cyber

Checkliste: Risiken und Lösungen

CYBER-VERSICHERUNG FÜR UNTERNEHMEN

CYBERSICHERHEIT: IHRE RISIKO-CHECKLISTE

Als Unternehmen sind Sie Cyberrisiken nicht schutzlos ausgeliefert – IT- und Cyber-Sicherheit sind möglich. Setzen Sie in einem ersten Schritt auf ein angepasstes IT-Sicherheitskonzept, das den Risiken und den Sicherheitsbedürfnissen Ihres Unternehmens gerecht wird. Das Restrisiko wiederum fängt eine maßgeschneiderte Cyber-Police auf: Schadensersatzansprüche, Ertragsausfall, Kosten für forensische Untersuchungen, PR-Beratung und Wiederherstellungskosten – Markel Pro Cyber schützt Sie vor den Folgen von Datenverlusten durch Hacker, betrügerische Erpressung und Betriebsausfälle.

TECHNISCHE SICHERHEIT: IHR RISIKO – IHRE LÖSUNG

1. DATENSICHERHEIT UND -WIEDERHERSTELLUNG

Ihr Risiko

Datensicherung und zeitnahe Datenwiederherstellung sind das A und O für Ihre technische Sicherheit. Ein Back-up-Laufwerk ist alternativlos: Damit wird Ihr Sicherheitsrisiko kalkulierbar – und bleibt bezahlbar.

Ihre Lösung

Ein Back-up-System, eingebettet in eine effiziente Sicherheitsstrategie, bildet die Basis für Ihre Sicherheit und die Voraussetzung für den Abschluss einer Versicherung im IT-Bereich.

2. ZUTRITT ZUM EDV-BEREICH

Ihr Risiko

Risiken lauern leider auch in den eigenen Reihen. Deshalb ist es relevant, dass Sie den Zutritt fremder und eigener Mitarbeiter zum EDV-Bereich gleichermaßen kontrollieren.

Ihre Lösung

Sicherheitszonen, physische Zutrittsbeschränkungen und Kontrollen sowie Regelungen für mobile und/oder Telearbeitsplätze minimieren das Risiko deutlich.

3. UNTERBRECHUNG DER STROMVERSORGUNG (USV)

Ihr Risiko

Gerade wenn Ihr Unternehmen im Netz verfügbar sein muss, ist eine unterbrechungsfreie Stromversorgung unabdingbar. Eine herkömmliche Notstromversorgung reicht hier nicht aus.

Ihre Lösung

Zur Sicherstellung Ihrer unternehmenskritischen Datenverarbeitungsbereiche oder laufenden Vorgänge ist die Anschaffung einer unterbrechungsfreien Stromversorgung (USV) mit passender Batteriekapazität empfehlenswert.

4. NETZTOPOLOGIE

Ihr Risiko

Wie Sie Ihr IT-Netz aufbauen und verwalten ist sicherheitsrelevant – und hängt neben den Kosten entscheidend von Kriterien wie Einfachheit, Sicherheit und Variabilität ab. Die Wahl des passenden Dienstleisters braucht daher Umsicht.

Ihre Lösung

Je nach Anforderung machen Einzelrechneranbindungen (Einzelzugang ohne individuelle E-Mail-Adresse für alle Mitarbeiter), ein Anschluss des Intranets an das Internet oder der arbeitsbedingte Zugriff interner Abteilungen auf das Internet (erfordert hohen administrativen Aufwand) Sinn.

5. SOFTWARE

Ihr Risiko

Als Unternehmen müssen Sie sich vor allem gegen Viren, Würmer und Trojanische Pferde aus dem Netz wappnen, um dem Ausspähen sensibler Daten – aber auch einer Betriebsunterbrechung wegen Nichterreichbarkeit bei Virenbefall – entgegen zu wirken.

Ihre Lösung

Nutzen Sie regelmäßig die kostenlosen Programme (Sicherheits-Patches) der Softwarehersteller, die Fehler (Bugs) großer Anwendungsprogramme reparieren. Achten Sie beim Download auf zuverlässige Quellen und auf Aktualität.

Besuchen Sie uns Online unter
www.markel.de/cyber-versicherung

CYBER-VERSICHERUNG FÜR UNTERNEHMEN

IT-SICHERHEIT: IHRE CHECKLISTE FÜR DIE CYBER-VERSICHERUNG

IT-Sicherheit ist der erste Schritt zur Unternehmenssicherheit. Und Voraussetzung für den Abschluss einer Cyber-Police – der letzte Schritt zur Cyber-Sicherheit. Doch welche etablierten IT-Schutzmaßnahmen werden im Antragsmodell abgefragt? Ein Überblick.

1. VIRENSCHUTZ MIT AUTOMATISCHEN UPDATES

Beim Virenschutz sind vor allem zwei Dinge relevant:

- Desktop Computer, Laptops und Terminals müssen mit einem Antivirenprogramm, Virenscanner oder Virenschutzprogramm (AV) ausgestattet sein. Das AV muss sowohl auf Clients als auch auf allen Server-Systemen laufen, auf denen Dateien gespeichert und verarbeitet werden, da diese mit Schadsoftware infiziert sein könnten.
- Das installierte AV muss immer auf dem aktuellen Stand sein. Das ist gewährleistet, wenn der Virenschutz als sogenannter Echtzeitscanner – sprich mit einer Auto-, Internet- oder auch Live-Updatefunktion – arbeitet: aktuelle Virensignaturen werden automatisch beim Hersteller heruntergeladen.

2. FIREWALLS AN SCHNITTSTELLEN

Besonders Schnittstellen zwischen internen und externen Netzen – beispielsweise zwischen firmeninternem Netz und Internet – müssen durch wirksame, individuelle Firewall-Strukturen an jedem Netzübergang betrieben werden. Nur so können nicht erwünschte Kommunikationsverbindungen zwischen beiden Netzen ausgeschlossen werden, indem das System den Kommunikationsfluss kontrolliert und filtert. Besonders sensible Netzbereiche sollte die Firewall ganz voneinander trennen.

3. PERMANENTE OFFLINE-DATENSICHERUNG

Datensicherung ist essenziell. Dafür sind Mindeststandards einzuhalten, die bestenfalls noch erweitert werden.

- Die Basis: Es ist mindestens eine vollständige Offline-Datensicherung (ausgesteckte externe Festplatte(n) oder sicher verwahrte Back-up-Bänder) etabliert, die nicht älter als eine Woche ist, damit eine Wiederherstellung sämtlicher kritischer Daten beziehungsweise Anwendungen für die Aufrechterhaltung des Geschäftsbetriebes möglich ist.
- Die Ergänzung: Optional ist es sinnvoll und üblich, stets zwei vollständige Back-ups offline und physisch vom IT-System getrennt vorzuhalten – falls eine Datensicherung einmal ausfällt bzw. nicht erfolgreich war, bleibt immer noch das zweite Back-up, um die Geschäftsfähigkeit aufrecht zu erhalten.

4. DOPPELTE ABSICHERUNG BEI FERNZUGRIFF

Um Fernzugriffe – Remote-Zugänge zu E-Mail-Konten oder auf Remote-Desktops aus dem Home Office oder im Rahmen von Telearbeit – so sicher wie nur möglich zu halten, stellt die Zwei-Faktor-Authentifizierung eine notwendige Sicherheitsmaßnahme dar. Sie verhindert beispielsweise den unberechtigten Zugriff auf E-Mail-Konten durch gestohlene Passwörter. Neben der doppelten Sicherheit schützt die Absicherung von Remote-Zugängen durch einen zweiten Faktor auch vor den Folgen von Phishing, Pharming, Brute-Force-Attacken und anderen Angriffsszenarien.

5. NEUE PASSWÖRTER & PINS FÜR TELEFONANLAGEN

Es ist erforderlich, dass für Telefonanlagen und Anrufbeantworter neue, individuelle Passwörter und PINs eingerichtet werden. Das heißt: Vorhandene bzw. voreingestellte Passwörter und PINs müssen geändert werden. Die Vorgehensweise variiert je nach Anlage – Informationen dazu sollten sich in den jeweiligen Nutzerhandbüchern finden. Unter Umständen können die notwendigen Informationen zum Änderungsprozess auch bei den Dienstleistern, die Ihre Anlage eingerichtet haben, erfragt werden.

6. RECHTEKONZEPT FÜR MITARBEITER & IT-VERANTWORTLICHE

Ein wichtiger Aspekt in der IT-Sicherheitskultur ist es, ein abgestuftes Rechtekonzept zu etablieren. Das bedeutet, dass Zugriffsberechtigungen nicht pauschal, sondern nach Verantwortlichkeit und Ressourcen definiert und vergeben werden.

- Abhängig von der Unternehmensgröße muss ein angemessenes Berechtigungskonzept umgesetzt sein, so dass jeder Mitarbeiter nur auf die Ressourcen Zugriff hat, die für das jeweilige Aufgabenspektrum benötigt werden.
- Ein IT-Administrator braucht ein abgestuftes Rechtekonzept mit administrativen Kennungen: Bei nicht-systemrelevanten Aktivitäten – dazu zählen u. a. Internetrecherche oder E-Mail-Bearbeitung – darf er keine administrativen Berechtigungen erhalten.

Ausnahme Einzelunternehmer: Einzelunternehmer mit nur einem Computer müssen lediglich ein separates Administrationskonto für Systemarbeiten wie Software-Installationen anlegen – die allgemeine Arbeit kann über ein Benutzerkonto mit eingeschränkten Rechten erfolgen.

Besuchen Sie uns Online unter
www.markel.de/cyber-versicherung

Markel Insurance SE
Schweizer Zweigniederlassung

Limbergstrasse 34,
8700 Küsnacht
Telefon: +41 (0) 58 25560 – 50

www.markel.ch
service@markel.ch

MARKEL®