



Sicherheit als Teil des Unternehmenskonzeptes.

Höchstmögliche Sicherheit ergibt sich aus dem Zusammenwirken dreier Faktoren: dem technischen, dem organisatorischen und dem personellen Faktor. Je besser diese drei auf das Gefährdungspotenzial aller Systeme und Applikationen, Geschäftsprozesse und Daten abgestimmt sind, desto wirksamer wird deren Schutz sein. Selten ist es mit einer vorgeschobenen Firewall und einem angehängten Anti-Virenprogramm getan. Wirksamer Schutz ist immer das Ergebnis einer sorgfältigen Beratung. Eben Consulting with Care.

Der technische Faktor.

Früher war alles einfacher. Es gab einen Zentralrechner und somit auch nur einen Angriffspunkt. Dann kam die Zeit der Client/Server-Systeme. Daten waren sofort und überall schnell verfügbar, Prozesse wurden schneller und komplexer.

Keine IT-Infrastruktur, die heute nicht auf diesem Prinzip aufbaut. Dies erfordert Sicherheitskonzepte, welche dieser Komplexität und den zahlreicher gewordenen Angriffspunkten gerecht werden. Heute, im Zeitalter des Internets und mit dem Aufkommen des Intranets, gilt es, die Informationen nicht nur im Unternehmen zu schützen, sondern auch, wenn diese zwischen mehreren Unternehmensstandorten und mobilen Mitarbeitern ausgetauscht werden.

Der organisatorische Faktor.

Sicherheit betrifft Ihr gesamtes Unternehmen. Ihr Gebäude und deren Zugangssysteme sind beispielsweise ebenfalls in Sicherheitskonzepten zu berücksichtigen. Ein- und ausgehende Dritte müssen kontrolliert werden und dürfen sich nur in festgelegten Bereichen bewegen.

Auch Mitarbeiter und deren Arbeitsmittel unterliegen unterschiedlichen Sicherheitsstufen. Manchmal ist der Einsatz von Chipkarten angebracht. Regeln beziehungsweise Verfahren für eintretende und besonders für scheidende Mitarbeiter sind zu definieren und über deren Einhaltung ist zu wachen.

Was geschieht bei Hackerangriffen, Viren oder Diebstahl? Was bei Ausbruch von Feuer und einem zu räumenden Gebäude? Was hat mit einem ausgemusterten oder defekten Rechner zu geschehen? Für alles werden Pläne benötigt und deren Inhalte und Verhaltensanweisungen sind den jeweiligen Mitarbeitern bekannt zu machen.

Der personelle Faktor.

Mitarbeiter müssen für das Thema Sicherheit und dessen Bedeutung für das gesamte Unternehmen sensibilisiert werden. Gut informierte, disziplinierte Mitarbeiter, welche Verhaltensregeln beachten, sind im Umgang mit unternehmenskritischen Daten der kostengünstigste Schutz.

Schutz wovor?

Nahezu jeder Geschäftsprozess basiert auf der Vernetzung verschiedenster, an das Internet angebundene, Rechner. Worin bestehen nun die Bedrohungen für Ihr Unternehmen? Aktive und passive Angriffe. Sie bestehen in Form passiver Angriffe (mit dem Ziel, durch Mitlesen an sensitive Daten zu gelangen) und in Form aktiver Angriffe (die in Ihre Datenübertragung eingreifen, diese stören oder Daten selbst modifizieren oder zerstören; Würmer einschleusen, oder, von Ihren Rechnern aus, eine falsche Identität vortäuschen). Auf diese Art Gefahren kann schnell reagiert und angemessen

und wirksam mit technischen Mitteln begegnet werden.

Unabsichtlich herbeigeführte Bedrohungen.

Daneben existiert für Ihr Unternehmen auch eine Bedrohung von innen. Von eigenen Mitarbeitern ausgehend. Fahrlässigkeit, Fehlbedienung und fehlendes Wissen im Umgang mit sensiblen Daten und Systemen sind in der Praxis die häufigste Ursache für Systemabstürze und Datenverluste. Einfache Abhilfe schaffen hier schriftliche Richtlinien zum Umgang mit kritischen Daten, die Mitarbeitern optimalerweise bei Eintritt in das Unternehmen ausgehändigt werden. Im Bedarfsfall gekoppelt mit erforderlichen Schulungen.

Unverzichtbar in beiden Fällen ist eine regelmäßige Datensicherung. Vor-Ort oder per Fernwartung - unabhängig, wie redundant Ihre Systemarchitektur ausgelegt ist. Ebenso unverzichtbar wie das Vorhandensein einer umfassenden Dokumentation, sowie eines Notfallplanes der Maßnahmen und Verantwortlichkeiten klar benennt.

Wir tun, was wir können.

Sicherheit ist ein sehr komplexes Thema. Wir von COWIC beraten Sie nicht nur in allen Fragen und begleiten Sie bei der Entscheidungsfindung, sondern offerieren Ihnen neben der Implementierung auch Betrieb und Wartung. Nutzen Sie unsere Leistungen wo Ihre Ressourcen an Wissen, Arbeitskraft, Sicherheit und technischer Ausstattung nicht ausreichen, Ihre Ansprüche angemessen umzusetzen.

Wir:

- stehen Ihnen hierbei gerne von der Planung von Sicherheitsstrategien und -konzepten,
- der Optimierung von IT-Prozessen bis zur erfolgreichen Implementation zur Seite.
- sorgen für störungsfreien Betrieb.
- erstellen Notfallpläne und Dokumentationen.
- beraten Sie bei der Auswahl und Beschaffung erforderlicher und geeigneter technischer Ausstattung.
- helfen bestehende Anwendungen zu integrieren.
- entwickeln und programmieren Sonderfunktionen und Schnittstellen.
- schulen Ihre System-Administratoren und Mitarbeiter.
- übernehmen auf Wunsch den laufenden Betrieb und die Wartung einschließlich Datensicherung.
- helfen Ihnen bei IT-Alltagsproblemen (zB. VoIP, Viren- und Spamfilter, Fernwartung, Serverbetrieb).

