A. Lehmann Elektro AG
Tellstr. 4
CH-9200 Gossau

Telefon 071 388 11 22
Telefax 071 388 11 21

info@lehmann.ch
www.lehmann.ch

Degersheimerstr. 74a
CH-9100 Herisau

Telefon 071 350 13 33
Telefax 071 350 13 34

herisau@lehmann.ch

MWST-Nr. 166 601

Zertifikat-Nr. 70143

Datensicherheit in der Unternehmung

Ein Leitfaden zur Erhöhung der Sicherheit und Verfügbarkeit von Einrichtungen zur Informationsverarbeitung in Unternehmungen

1 Inhaltsverzeichnis

2 Das Umfeld

2.1 Nutzung der Informationstechnologie

Informationstechnologie – kurz IT - ist aus unserem Leben nicht mehr wegzudenken. Praktisch alle Geschäftsprozesse beziehen und liefern Daten, die elektronisch verarbeitet werden. Die meisten Datenaufzeichnungen sind heute elektronisch.

Das heisst aber auch, dass – wenn die IT ausfällt – Prozesse gestört sind und Aufzeichnungen fehlen. In vielen Unternehmungen ist man sich dieser Tatsache bewusst, es kommt aber auch vor, dass die Auswirkungen massiv unterschätzt werden. Klar zum Ausdruck kommen diese Auswirkungen spätestens bei einem Systemausfall, die damit verbundenen Aufwendungen und Kosten sind unter Umständen gewaltig.

Die elektronische Aufzeichnung von Daten bringt auch mit sich, dass diese Daten verändert, kopiert, gelöscht oder unbrauchbar gemacht werden können, ohne dass diese Tatsache unmittelbar bemerkt wird. Die Suche nach der Ursache der Datenmanipulation gestaltet sich schwierig, in vielen Fällen ist sie gar nicht eruierbar.

Es gibt nur einen Weg, die Sicherheit in der Informationstechnologie zu erhöhen, und dieser besteht darin, sich der Risiken bewusst zu werden und seine Systeme so zu schützen, dass Fehler weitgehend ausgeschlossen werden können und dass im Fehlerfall der Schaden begrenzt bleibt.

2.2 Die Vernetzung

Internet ist eine gute Sache. Es vereinfacht viele Arbeiten, es ist eine kostengünstige Kommunikationsmethode und es ist effizient. Es hat aber auch den Einfluss, dass Telekommunikation und Datenkommunikation zusammenwachsen, dass unsere Internet-Arbeitsplätze Teil eines weltumspannenden Netzwerkes sind und damit von aussen ansprechbar, empfangsbereit für nützliche Informationen, aber leider auch für alles andere. Vernetzung ist die Grundlage für die moderne Sabotage an Dateneinrichtungen. Entsprechend hat die Anzahl von Attacken auf Unternehmungen, die ihren Ursprung nicht in der Unternehmung selbst haben, mit dem Einsatz des Internet sprunghaft zugenommen.

2.3 Risiken

Wer Systeme sicher gestalten will, muss sich im Klaren sein, welche Gefahren lauern. Bei der Frage der Sicherheit in IT-Systemen lassen sich diese Risiken in Klassen einteilen.

1. *Umweltrisiken*
2. *Risiken in der Organisation*
3. *Risiko Datenverlust und Datenmanipulation*
4. *Risiko Systemausfall*

Innerhalb der Klassen bestehen eine Anzahl definierter Risiken, zu denen sich Massnahmen definieren lassen. Die Risiken lassen sich erkennen, indem man sich die Fragen aus der folgenden Checkliste stellt.

3 Checkliste Risiken

Risikoklasse	*Risiko*	*Frage*	*ja*	*nein*	*zugehöriges Massnahmen -papier*
1 Umwelt	Wasser	Sind meine Geräte vor einem Wassereinbruch geschützt oder wird ein eventueller Wassereinbruch gemeldet?	**q**	**q**	U101
1 Umwelt	Feuer	Sind meine Geräte an einem feuersicheren Ort untergebracht?	**q**	**q**	U102
1 Umwelt	Feuer/Wasser	Sind meine Backup-Medien an einem separaten Ort (oder an mehreren Orten) untergebracht?	**q**	**q**	U120
1 Umwelt	Elektrische Versorgung	Gibt es Notstromversorgungen für die Überbrückung kurzzeitiger Ausfälle und für die geregelte Systemabschaltung?	**q**	**q**	U121
1 Umwelt	Elektrische Versorgung	Gibt es einen Notfallplan für das Arbeiten ohne Netzversorgung?	**q**	**q**	U128
1 Umwelt	Elektrische Versorgung	Sind die Systeme ausreichend gekühlt und steigt die Umgebungstemperatur auch im Sommer nicht zu stark an?	**q**	**q**	U140
2 Organisation	Führung	Ist Das Thema „Datensicherheit in der Unternehmung“ ein Traktandum in der Unternehmensleitung und wird das Thema regelmässig behandelt?	**q**	**q**	O101
2 Organisation	Führung	Existiert eine dokumentierte IT-Politik der Unternehmensleitung?	**q**	**q**	O102
2 Organisation	Führung	Wird beim Start neuer Projekte und während dem Ablauf dem Thema IT-Sicherheit Beachtung geschenkt?	**q**	**q**	O103
2 Organisation	Führung	Sind die internen Weisungen und Richtlinien einfach und für die Mitarbeitenden verständlich ?	**q**	**q**	O104
2 Organisation	Führung	Sind die Zuständigkeiten und Stellvertretungen klar geregelt ?	**q**	**q**	O105
2 Organisation	Führung	Wird die IT-Sicherheit in regelmässigen Abständen kontrolliert ?	**q**	**q**	O106
2 Organisation	Führung	Wird die Qualität des IT-Supportdienstes regelmässig kontrolliert ?	**q**	**q**	O107
2 Organisation	Raumschutz	Sind Server- und zentrale IT-Systeme in separaten, abschliessbaren Räumen untergebracht?	**q**	**q**	O150
2 Organisation	Raumschutz	Ist der Zugang zu Server- und zentralen IT-Systemen geregelt?	**q**	**q**	O151

Risikoklasse	*Risiko*	*Frage*	*ja*	*nein*	*zugehöriges Massnahmen -papier*
2 Organisation	Ordnung	Herrscht Ordnung in der Dokumentation der IT-Systeme?	**q**	**q**	O201
2 Organisation	Ordnung	Existiert eine aktualisierte Dokumentation und Inventarisierung der IT-Systeme ?	**q**	**q**	O202
2 Organisation	Ordnung	Ist die erforderliche Anzahl von Lizenzen für Softwareprodukte (Betriebssysteme, Anwenderprogramme) vorhanden?	**q**	**q**	O210
2 Organisation	Wartung	Werden notwendige Sicherheits-Updates und Patches regelmässig eingespielt, und werden die Aktivitäten protokolliert ?	**q**	**q**	O221
2 Organisation	Wartung	Geschehen Wartungs- und Reparaturarbeiten nach definierten Abläufen ?	**q**	**q**	O222
2 Organisation	Wartung	Existieren Notfall-Checklisten, die es ermöglichen, Systeme auch dann wieder in Gang zu setzen, wenn der Systemverantworliche nicht verfügbar ist?	**q**	**q**	O223
2 Organisation	Mitarbeiter	Sind die Rechte für Datenzugriff für jeden Mitarbeiter definiert?	**q**	**q**	O231
2 Organisation	Mitarbeiter	Ist sichergestellt, dass Mitarbeiter nicht auf Daten zugreifen können, die nicht mit ihrem Arbeitsfeld zu tun haben?	**q**	**q**	O232
2 Organisation	Mitarbeiter	Hat jeder Mitarbeiter einen Benutzernamen und ein Passwort?	**q**	**q**	O233
2 Organisation	Mitarbeiter	Werden sichere Passwörter verwendet?	**q**	**q**	O234
2 Organisation	Mitarbeiter	Werden Passwörter periodisch geändert?	**q**	**q**	O235
2 Organisation	Mitarbeiter	Werden Benutzerkonten von Mitarbeitern, die die Unternehmung verlassen, gelöscht ?	**q**	**q**	O236
2 Organisation	Mitarbeiter	Ist sichergestellt, dass ausser dem Systemverantwortlichen niemand Administratorenrechte auf den Servern besitzt?	**q**	**q**	O240
2 Organisation	Mitarbeiter	Ist das Administratorenpasswort wirklich nur dem Systemverantwortlichen bekannt?	**q**	**q**	O241
2 Organisation	Mitarbeiter	Gibt es einen Zuständigen für die Datensicherungen und werden die Aktivitäten protokolliert?	**q**	**q**	O242
2 Organisation	Mitarbeiter	Werden die Mitarbeitenden regelmässig geschult ?	**q**	**q**	O243
2 Organisation	Mitarbeiter	Werden die internen Weisungen und Richtlinien durch alle Mitarbeitenden konsequent befolgt ?	**q**	**q**	O250
2 Organisation	Fernzugriff	Wissen Sie, welche Möglichkeiten bestehen, um von extern auf ihr Firmennetzwerk zuzugreifen?	**q**	**q**	O300
2 Organisation	Fernzugriff	Wissen Sie, welche Personen von extern Zugang zum Firmennetzwerk haben ?	**q**	**q**	O301

Risikoklasse	*Risiko*	*Frage*	*ja*	*nein*	*zugehöriges Massnahmen -papier*
2 Organisation	Fernzugriff	Werden Zugangskonten von Personen gelöscht, die künftig keinen Zugang mehr von extern haben sollen ?	**q**	**q**	O302
2 Organisation	Fernzugriff	Ist der Zugang von extern durch Passwörter und Call-Back-Verfahren gesichert ?	**q**	**q**	O303
2 Organisation	Fernzugriff	Ist die Möglichkeit des Fernzugriff zeitlich limitiert?	**q**	**q**	O304
2 Organisation	Fernzugriff	Ist die Konfiguration von Geräten für den Fernzugriff (Router, Gateways etc.) durch sichere Passwörter geschützt ?	**q**	**q**	O305
2 Organisation	Fernzugriff	Ist sichergestellt, dass nach einer bestimmten Anzahl von Einwählversuchen mit falscher Identität der Zugang gesperrt ist ?	**q**	**q**	O306
2 Organisation	Fernzugriff	Sind Sicherheitseinrichtungen (Firewalls) im Einsatz, die die Möglichkeiten von Fernzugriffen auf das Erwünschte limitieren ?	**q**	**q**	O307
3 Datensicherheit	Datensicherung	Gibt es eine festgelegte Strategie zur Datensicherung ?	**q**	**q**	D101
3 Datensicherheit	Datensicherung	Existiert eine Planung für Datensicherungen?	**q**	**q**	D102
3 Datensicherheit	Datensicherung	Ist sichergestellt, dass alle relevanten Daten gesichert werden ?	**q**	**q**	D110
3 Datensicherheit	Datensicherung	Existieren Aufzeichnungen über Datensicherungen und sind diese geordnet abgelegt?	**q**	**q**	D111
3 Datensicherheit	Datensicherung	Werden Datenträger für Sicherungen an getrennten Orten aufbewahrt ?	**q**	**q**	D112
3 Datensicherheit	Datensicherung	Ist der Aufbewahrungsort für Datenträger für Sicherungen vor Fremdzugriff geschützt ?	**q**	**q**	D113
3 Datensicherheit	Datensicherung	Sind Datenträger für Sicherungen dauerhaft und eindeutig gekennzeichnet ?	**q**	**q**	D114
3 Datensicherheit	Datensicherung	Ist sichergestellt, dass Datenbanken, die im Sicherungszeitpunkt in Bearbeitung sind, dennoch gesichert werden ?	**q**	**q**	D115
3 Datensicherheit	Datensicherung	Ist sichergestellt, dass lokal abgelegte Daten von Wichtigkeit ebenfalls gesichert werden ?	**q**	**q**	D116
3 Datensicherheit	Datensicherung	Wird periodisch überprüft, ob die Daten auf den Datenträgern für die Sicherung auch tatsächlich vollständig sind ?	**q**	**q**	D120
3 Datensicherheit	Datensicherung	Wird periodisch überprüft, ob Daten von den Datenträgern für die Sicherung auf die Systeme zurückgesichert werden können und die Daten danach auch gültig sind ?	**q**	**q**	D121
3 Datensicherheit	Datensicherung	Gibt es einen Verantwortlichen für die Datensicherung ?	**q**	**q**	D150

Risikoklasse	*Risiko*	*Frage*	*ja*	*nein*	*zugehöriges Massnahmen -papier*
3 Datensicherheit	Datensicherung	Ist die lückenlose Stellvertretung des Sicherungsverantwortlichen geregelt ?	**q**	**q**	D151
3 Datensicherheit	Datensicherung	Werden alle Tätigkeiten in Zusammenhang mit der Datensicherung protokolliert ?	**q**	**q**	D160
3 Datensicherheit	Internet	Ist eine Firewall zwischen Internet und Unternehmensnetzwerk geschaltet?	**q**	**q**	D201
3 Datensicherheit	Internet	Ist die Firewall aktiviert und bietet sie genügenden Schutz ?	**q**	**q**	D202
3 Datensicherheit	Internet	Besitzen Router und Firewalls sichere Passwörter ?	**q**	**q**	D203
3 Datensicherheit	Internet	Sind Mitarbeiter im Umgang mit dem Internet geschult und sensibilisiert ?	**q**	**q**	D204
3 Datensicherheit	Internet	Besteht eine betriebsinterne Richtlinie für den Umgang mit dem Internet ?	**q**	**q**	D205
3 Datensicherheit	Viren etc.	Ist ein Virenschutz auf allen Arbeitsplätzen installiert ?	**q**	**q**	D301
3 Datensicherheit	Viren etc.	Ist ein Virenschutz auf allen Servern installiert ?	**q**	**q**	D302
3 Datensicherheit	Viren etc.	Besteht ein gültiger Lizenzvertrag mit dem Anbieter der Virenschutzsoftware?	**q**	**q**	D303
3 Datensicherheit	Viren etc.	Wird der Antivirenschutz periodisch (idealerweise täglich) mit einem Update über Internet versehen?	**q**	**q**	D304
3 Datensicherheit	Viren etc.	Sind die Mitarbeiter im Umgang mit dem Virenschutzprogramm instruiert ?	**q**	**q**	D310
3 Datensicherheit	Software	Sind aktuelle Sicherheitspatches für Anwenderprogramme (Office-Produkte, Web-Browser, Mail-Clients) im Einsatz und wird deren Aktualität laufend überprüft?	**q**	**q**	D401
3 Datensicherheit	Software	Sind die in Anwendungen eingebauten Schutzmechanismen aktiviert und können durch Mitarbeitende nicht ausser Kraft gesetzt werden ?	**q**	**q**	D402
3 Datensicherheit	Software	Sind Standard-Passwörter von Softwarepaketen durch sichere Passwörter ersetzt worden ?	**q**	**q**	D403
4 Systemausfall	Hardware-Ausfall	Sind die Daten redundant abgelegt ?	**q**	**q**	S101
4 Systemausfall	Hardware-Ausfall	Ist die Datensicherung so ausgelegt, dass im Falle eines Systemausfalls auf ein Ersatzsystem rückgesichert werden kann?	**q**	**q**	S201
4 Systemausfall	Hardware-Ausfall	Sind die allerwichtigsten Ersatzteile im Haus an Lager?	**q**	**q**	S202
4 Systemausfall	Hardware-Ausfall	Sind die eingesetzten Hardwareteile noch erhältlich und bietet der Hersteller Ersatzteilgarantie?	**q**	**q**	S203
4 Systemausfall	Hardware-Ausfall	Lassen sich Ersatzteile in vernünftiger Frist beschaffen?	**q**	**q**	S204
4 Systemausfall	Hardware-Ausfall	Bietet mein Systemsupporter Ersatzteilgarantie ?	**q**	**q**	S205

Risikoklasse	*Risiko*	*Frage*	*ja*	*nein*	*zugehöriges Massnahmen -papier*
4 Systemausfall	Hardware-Ausfall	Bietet mein Systemsupporter ein Ersatzsystem ?	q	q	S206
4 Systemausfall	Hardware-Ausfall	Gibt es für die Zeit des Systemausfalls ein Notsystem für die wichtigsten Arbeiten ?	q	q	S207

4 Massnahmen-Papiere