Psychische Belastungen evaluieren

„Sicherheit ist wirtschaftlich!“ – auch wenn es auf den ersten Blick nur nach Aufwand und Kosten aussieht. Die rechtlichen Anforderungen werden nicht geringer, sondern zunehmend schärfer und aufwändiger.

Foto: Thinkstock

Für die Evaluierung sehr bewährt haben sich Gruppen-Workshops, die durch entsprechend ausgebildetes Personal moderiert werden.

Durch die Arbeitsplatzevaluierung (Ermittlung und Beurteilung von Gefahren und Belastungen sowie Festlegung von technischen und organisatorischen Maßnahmen) ist in der Regel schon ein gutes Fundament für die Sicherheitsarbeit im Unternehmen gelegt. Herkömmliche Verfahren hatten dabei aber die Stressfaktoren, insbesondere die psychischen Belastungen häufig nicht oder zu wenig berücksichtigt. Aufgrund der letzten Novelle des Arbeitnehmerschutzgesetzes (ASchG BGBl. Nr. 450/1994), veröffentlicht mit BGBl. I Nr. 71/2013 ist die Durchführung der „Evaluierung psychischer Belastungen“ nun eine zwingende Forderung geworden. Dabei soll durch besondere Methoden herausgearbeitet werden, wo die in Zusammenhang mit der Arbeit verbundenen eigentlichen „Stressfaktoren“ liegen und welche Maßnahmen erforderlich sind, um diese Stressfaktoren zu erkennen und zu vermeiden. Erwähnenswert ist, dass bei der „Evaluierung psychischer Belastungen“ um interne Abläufe, Prozesse, Verfahren und die verschiedenen Kommunikationsformen geht. Die Präventivdienste (Arbeitsmediziner Sicherheitsfachkräfte etc.) müssen zu diesem Prozess hinzugezogen werden.

„Der Nutzen der Evaluierung psychischer Belastungen liegt sowohl auf der Seite der Beschäftigten sowie auf der Seite des Beschäftigers. Also eine klassische Win-Win-Situation“, betont Johannes Rigg, Berufsgruppensprecher der Sicherheitsfachkräfte. Die Berufsgruppe der Sicherheitsfachkräfte in der FG der gewerblichen Dienstleister unterstützt Klein-, Mittel- und Großbetriebe bei der Umsetzung dieser rechtlichen Anforderung und stellen heraus, dass „Sicherheit wirtschaftlich ist“.

Windows XP ist ein unsicheres Betriebssystem

Nach zwölf Jahren, sechs Monaten und zwölf Tagen ist es eingetroffen: Das Ende des erweiterten Supports von Windows XP mit 8. April 2014.

Damit liefert Microsoft für dieses langgediente Betriebssystem keine Updates mehr und auch Sicherheitslöcher werden nicht mehr gestopft. Der Termin war überraschend wie Weihnachten, dennoch sind noch sehr viele Rechner mit Windows XP im aktiven Betrieb. Ist das bedenklich oder vielleicht sogar fahrlässig?

Welche Gefahren bestehen? Auch bei dem langgedienten Betriebssystem tauchten bis zu letzt immer wieder Sicherheitsrisiken auf, die durch Patches behoben wurden. Solche Löcher können ausgenutzt werden, um in Systeme einzudringen, Daten zu stehlen oder die Geräte für unerwünschte Dinge einzusetzen. Stellen Sie sich vor, Ihr Rechner würde verwendet um Kinderpornografie zu verbreiten! Manche Sicherheitsspezialisten nehmen an, dass von Hackern längst bekannte Sicherheitslücken geheim gehalten wurden, um diese nun nach dem Ende des Supports unbehelligt auszunutzen.

Ihre IT-Sicherheitstipps

exklusiv von den IT-Security-Experts

Die einfache Aussage ist: Ersetzen Sie alle Windows XP Rechner durch neue mit Windows 7 oder 8. Das gleiche gilt übrigens auch für Windows Server 2003 und Office 2003. Bei Rechnern jüngeren Datums kann ein Upgrade auf Windows 7 durchgeführt werden. Ältere Rechner sollten jedoch komplett durch aktuelle, performante und möglichst sparsame Rechner ersetzt werden.

Falls Sie einzelne Rechner mit veralteten Systemen noch nicht ersetzen können, sollten Sie einige Maßnahmen ergreifen:

- Alle Dienste und Programme, die nicht unbedingt benötigt werden abdrehen
- Sämtliche Updates installieren
- Den direkten Internetzugriff und Zugriff auf USB Datenträger verhindern

Microsoft bietet auch weiterhin Premium Supportverträge für Windows XP Kunden an. Diese sind jedoch kostenintensiv. Vor allem wenn tatsächlich Sicherheitsprobleme ohne aktuelle Lösungen behoben werden sollten.

Erfassen Sie möglichst rasch, welche Rechner in Ihrem Unternehmen noch mit den unsupporteten Betriebssystemen betrieben werden und klären Sie mit ihrem IT Betreuer die notwendigen Maßnahmen. Gerne unterstützen Sie die IT-Security-Experts dabei.

IT-Security-Expert Glojek.

IT-Security-Experts-Group

Georg Doern **www.its-doern.at**, Manuel Glojek **www.grasgruen.it**, Wolfgang Hödl **www.profit-management.at**, Horst Kasper **www.rescue.at**, Karl Obexer **www.obexer.at**, Roland Schaffer **www.schaffer-se.at**, Andreas Wieser **www.ideefix.eu**