**Cyberkriminalität – was ist denn das?**

**Mangelndes Risikobewusstsein an den Pranger gestellt**

**„Ich bin davon überzeugt, dass es nur zwei Arten von Unternehmen gibt: diejenigen, die schon gehackt wurden, und diejenigen, die noch gehackt werden.“ Dieses Zitat von FBI-Direktor Robert Mueller stand Pate für die von den Verbänden der Holz- und Möbelindustrie Nordrhein-Westfalen gemeinsam mit ihrem Kooperationspartner Allianz-Versicherungs AG initiierte November-Veranstaltung „Unternehmensrisiko Cyber Kriminalität“.**

Der Workshop in den Herforder Geschäftsräumen des Verbands war mit etwa 30 Gästen aus der Möbelbranche sehr gut besucht. Hintergrund der Tagung bildet die mit zunehmender Digitalisierung und Vernetzung von Geschäftsprozessen wachsende Gefahr für Unternehmen. Jene sind heute anfällig wie nie zuvor für Cyber-Attacken, Identitätsdiebstahl, Internet-Sabotage oder Datenverlust. Der Schaden durch Attacken von Online-Kriminellen wird auf jährlich rund 50 Milliarden Euro geschätzt.

**Cyberkriminalität kann existenzbedrohend sein**

Cyberkriminalität ist klar auf dem Vormarsch und stellt eine Bedrohung für alle Unternehmen dar, unabhängig von Größe oder Branche. Doch Systemausfälle und Datenverluste können auch interne Ursachen haben – wie mangelhafte Sicherheitsvorkehrungen, Bedienungsfehler oder auch Vorsatz durch Mitarbeiter. Auf Datenschutzverletzungen und Datenmissbrauch reagieren die Gesetzgeber mit immer strengeren Datenschutzregeln und hohen Bußgeldern, die für ein Unternehmen im Falle eines Schadens sogar existenzbedrohend sein können.

Der erste Teil der Veranstaltung stand ganz unter den Fragestellungen: Wie verbreitet ist Cyberkriminalität? Welche Risiken entstehen für meine Geschäftsprozesse und mein Unternehmen? Wo lauern die Gefahren, wie kann mein Unternehmen angegriffen werden? Welche Techniken werden verwendet? Welche Gefahren entstehen durch Mobile Devices? Wie kann ich meine Mitarbeiter für das Thema sensibilisieren? Und – last but not least: Wie kann ich mein Unternehmen wirklich schützen?

**Mit Sozialen Medien steigen die Risiken**

Als sachkundige Referentin konnte Dr. Anja Padberg gewonnen werden. Sie ist Mitgründerin und Gesellschafterin der Marcant GmbH aus Bielefeld – ein M2M Solution Provider und Internet Systemhaus mit internationaler Ausrichtung, welches auf Virtualisierungs- und Sicherheits-Lösungen, VPN- und Netzwerkmanagement bzw. -überwachung sowie mobile Lösungen mit UMTS/GPRS für Business- und M2M-Anwendungen spezialisiert ist.

Allein ihr wie beiläufig beigebrachtes Beispiel einer Schweizer Untersuchung, nachdem in Unternehmen pro Mitarbeiter und Jahr durchschnittlich rund 4 CHF für Toilettenpapier, hingegen nur etwas über 2 Franken für IT-Sicherheit aufgewendet werden, spricht programmatische Bände. Denn die Gefahren und leider ebenso die Einfallstore im Unternehmen für Angriffe sind gewaltig und wachsen weiter. Der Risikofaktor Mensch, dessen Spieltrieb und die – unternehmensseitig immer häufiger gewollte – Nutzung privater mobiler Endgeräte für die Arbeit potenzieren die Risiken.

**App-Klone und WLAN-Netze besonders gefährlich**

Gefährliche Dienstarten sind inzwischen so gut wie alle beliebten Grundnutzungen an Mobile Devices und Computern: Informationsspeicher, Informations-und Kommunikationsdienste, Multimedia-Nutzungen, Datentransfer bzw. Synchronisationen, GPS und Zellortung, Spiele, Spezialanwendungen für den Außendienst, die VPN-Zugänge und natürlich Online Banking, Bezahl- sowie Messagingdienste. Also nahezu alle Nutzungen, wofür mobile Geräte eigentlich beworben und gekauft werden. Mobile Malware hingegen, obgleich Deutschland Angriffsziel Nr. 2 weltweit ist, steht bisher gar nicht im Fokus der allgemeinen Risikowahrnehmung. Besonders kritisch: „äußerlich“ harmlose App-Klone, die dennoch Schadsoftware enthalten.

Die Auswirkung sind oft gravierend, wie z.B. der Diebstahl von privaten Daten, das Löschen von Informationen und Daten auf dem Telefon, das Entwenden von Passwörtern für Online-Banking oder vielleicht sogar die komplette Verhinderung des Zugriffs auf das Smartphone. Dr. Padberg gab schließlich eine Fülle anwendungsspezifischer Empfehlungen für die IT-Sicherheit in Unternehmen. Ihr spannender Vortrag schloss mit einer Livedemonstration zum Passwort-Cracking. Wie einfach erfolgreiches Hacking inzwischen für den Profi ist, war für viele der Gäste ein bisher einmaliges Erlebnis.

**Versicherungsschutz vor Cyber-Crime möglich und nötig**

Rund 70.000 Euro beträgt derzeit der Schadensdurchschnitt eines Hackerangriffs in Deutschland, über 60.000 Fälle wurden im vergangenen Jahr erfasst. Wie hoch liegt jedoch die Dunkelziffer? Mit diesem Aufschlag beklagten im zweiten Veranstaltungsteil Dr. Andreas Fürst und Jens Krickhahn von der Allianz-Versicherung das noch immer völlig unterentwickelte Risikobewusstsein für Cyberkriminalität – gewissermaßen vom Pförtner bis zum Vorstandsvorsitzenden.

Die Vertreter der Assekuranz stellten verschiedene Modelle vor, die maßgeschneidert Versicherungsschutz gegen Cyber-Risiken für alle Kundensegmente anbieten. Wichtige Fragen wie „Warum braucht es überhaupt eine eigenständige Cyberpolice?“ und „Wie reagieren meine traditionellen Versicherungen?“ wurden ausführlich erörtert. Denn eines wurde am Ende dieses interessanten Exkurses jedem Zuhörer klar: Technische und organisatorische Maßnahmen bieten keinen 100%igen Schutz gegen Cyber-Gefahren – es bleiben immer Restrisiken, die es zu (ver)sichern gilt. Es sei denn: Wir schalten das Internet dauerhaft ab…