PRESSEMITTEILUNG

Ein Viertel aller Mittelständler war bereits Opfer von Cyber-Kriminellen

Stuttgart, 13.10.2014 – Bereits zum zweiten Mal trafen sich Spitzen aus Wirtschaft, Wissenschaft und Politik im Internationalen Congresscenter Stuttgart, um sich über die Perspektiven des IKT-Standortes Baden-Württemberg auszutauschen. Im Rahmen der „Forward IT“ diskutierten sie über aktuelle Risikoszenarien und mögliche Lösungsansätze für mehr IT-Sicherheit. Der Schwerpunkt lag in diesem Jahr auf kleinen und mittelständischen Unternehmen (KMU).

Mittelständler sind von Angriffen auf ihre IT-Infrastruktur in gleichem Maße betroffen wie Konzerne, verfügen aber häufig nicht über das Bewusstsein, das Wissen und die finanziellen Mittel, um sich ausreichend zu schützen. „Die IT-Affinität in KMU ist ausgesprochen hoch“, sagte der Beauftragte der Landesregierung für Mittelstand und Handwerk, Peter Hofelich, auf der Forward IT. „Auf der anderen Seite ist das Budget für IT-Sicherheit hier besonders gering.“ Laut einer Studie des Bundesministeriums für Wirtschaft und Technologie liegt es bei 14 Prozent vom Gesamt-IT-Budget der Unternehmen. Auch die Dringlichkeit, mit der sicherheitsrelevante Vorfälle behandelt würden, liegt im Mittelstand unter dem Durchschnitt: Gerade einmal 5 Prozent der kleinen und mittleren Unternehmen meldeten einen sicherheitsrelevanten Übergriff auf ihre IT-Infrastruktur an die Behörden, berichtete Jürgen Fauth, Kriminaloberrat beim Landeskriminalamt – die meisten der Betroffenen melden diese Vorfälle aus Angst vor Reputationsverlust nicht.

Zahl und Schwere der Cyber-Angriffe deutlich gestiegen

Zugleich ist die Zahl erfolgreicher Cyber-Attacken deutlich gestiegen. „Sowohl die Menge als auch die Schwere der Angriffe hat in den vergangenen zwei Jahren dramatisch zugenommen“, erklärte Dirk Wittkopp, Geschäftsführer der IBM Research & Development GmbH. 25 Prozent aller KMU sind nach Angaben des Landeskriminalamtes in den vergangenen zwei Jahren Opfer einer Cyber-Attacke geworden. Experten gehen davon aus, dass sich die Zahl der Angriffe tendenziell noch erhöhen wird. Besorgniserregend seien in Zusammenhang mit IT-Sicherheit nicht so sehr die Aktivitäten von Hackern, sondern die organisierte Wirtschaftsspionage und die Cyber-Kriminalität. So habe sich in den letzten Jahren ein veritabler Schwarzmarkt für den Handel mit Datenpaketen entwickelt, betonte Cybercrime-Experte Fauth.

Neue Technologien zu meiden oder zu verbieten ist keine Option

Doch die Experten lieferten nicht nur eine Bestandsaufnahme der aktuellen Herausforderungen, sondern zeigten auch Lösungsansätze auf. Einig waren sich alle Anwesenden darin, dass ein integriertes IT-Sicherheitskonzept notwendig ist, um zukünftige Bedrohungen abzuwehren. Neue Technologien zu meiden oder gar zu verbieten, sei dabei keine Option, sagte Dirk Fox, Geschäftsführer von Secorvo Security Consulting und Mitglied des Vorstands beim Karlsruher CyberForum. Sie sinnvoll zu regeln und unter Umständen auch zu begrenzen, dagegen schon.

Entsprechende Initiativen dürften nicht allein von der IT-Abteilung ausgehen, sondern müssten als strategische Aufgaben begriffen werden. „IT-Sicherheit ist eine Querschnittsaufgabe, die Management, Recht und Informatik gemeinsam vorantreiben müssen“, sagte Prof. Dr. Andreas Oberweis vom Karlsruher Forschungszentrum Informatik (FZI). Darüber hinaus müsse auch das Netzwerk eines Unternehmens in die IT-Sicherheitsstrategie einbezogen werden. „Es reicht nicht aus, das eigene Unternehmen gegen Angriffe abzusichern“, sagte Dirk Wittkopp. Auch Partner und Zulieferer könnten Opfer einer Web-Attacke sein und unbeabsichtigt Malware in ein Unternehmen einschleusen. Generell gilt: Wer sich frühzeitig gegen einen möglichen Angriff rüstet, geht mit hoher Wahrscheinlichkeit ohne größeren Schaden aus einem Cyber-Angriff hervor.

Wer sich nicht ausreichend schützt, kann haftbar gemacht werden

Einig waren sich alle Experten darin, dass IT-Sicherheit künftig einen noch höheren Stellenwert in den Unternehmen einnehmen werde. „Wenn man gegenrechnet, was ein erfolgreicher Angriff die Unternehmen kostet, dann sind die Investitionen in IT-Sicherheit allemal gerechtfertigt“, sagte Dr. Simone Rehm, Leiterin des Zentralbereichs IT + Prozesse bei TRUMPF in Ditzingen. Nicht nur der finanzielle Verlust – laut einer Umfrage von Kaspersky Lab liegt er für KMU pro Angriff bei 70.000 Euro – kommt die Unternehmen teuer zu stehen. Auch der Imageverlust ist im Falle eines erfolgreichen Angriffs beträchtlich. Hinzu kommen rechtliche Risiken. Denn wer sich nicht ausreichend gegen einen Cyber-Angriff schützt, der kann im Zweifelsfall haftbar gemacht werden. „Sorglosigkeit im Umgang mit IT-Sicherheit kann zum Haftungsrisiko werden“, erklärte Dr. Dirk Heckmann, Professor für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau.

Land fördert IT-Sicherheit im Rahmen von Forward IT

Viele Unternehmen hätten inzwischen erkannt, dass IT-Sicherheit kein notwendiges Übel sei, sondern eine Investition in den Unternehmenswert. „Insofern hatte die NSA-Affäre auch etwas Gutes“, sagte Werner Bachmann, Leiter des Bereichs IT-Recht bei der Kanzlei Friedrich Graf von Westphalen & Partner. „Ein Sensibilisierungsprozess hat stattgefunden“,

bestätigte auch Simone Rehm. Viele Unternehmen seien sich der Risiken durch IT-Angriffe heute sehr viel bewusster als noch vor zwei Jahren. Zugleich wünschten sich die Experten, dass dem neuen Risikobewusstsein auch ein neuer rechtlicher Rahmen folge. „Durch die NSA-Affäre haben wir erstmals die Chance, zu einer modernen Datenschutzgesetzgebung zu kommen“, sagte Alf Henryk Wulf, Vorstandsvorsitzender der Wirtschaftsinitiative Baden-Württemberg: Connected e.V. (bwcon).

Auf Bundesebene könnte das IT-Sicherheitsgesetz die bisherige Lücke in der Gesetzgebung schließen. Auf Landesebene ist das Thema IT-Sicherheit fest im Plan der IKT-Allianz verankert. 33 Millionen Euro an Fördergeldern will die Landesregierung in den nächsten vier Jahren in die Weiterentwicklung des IKT-Standortes Baden-Württemberg investieren. Sicherheitsrelevante Projekte spielen dabei eine herausragende Rolle. Ab dem Jahr 2015 sollen zunächst 17 Millionen Euro fließen in Projekte zur IT-Sicherheit, Standortentwicklung, IKT als Querschnittstechnologie und die Digitalisierung der Anwenderbranchen. Beim Thema Sicherheit stehen der Ausbau des Forschungszentrums Informatik (FZI) in Karlsruhe zur zentralen IT-Sicherheitsagentur sowie das Kompetenzzentrum für IT-Sicherheit im Rahmen des beabsichtigten House of IT zunächst an erster Stelle. Damit hätten vor allem Mittelständler künftig eine Anlaufstelle, die ihnen beim Schutz vor Datenspionage und Datenmissbrauch beratend zur Seite steht.

Weiterführende Informationen

- Forward IT: www.ikt-bw.de
- Baden-Württemberg: Connected: www.bwcon.de
- IT & Business: http://www.messe-stuttgart.de/where-it-works/
- Bilder der Forward IT – Sicherheitskonferenz: http://bit.ly/forwardit2014
  Als Quellenangabe bitte bwcon/Uli Regenscheit angeben.

Über Baden-Württemberg: Connected e.V. (bwcon)

Baden-Württemberg: Connected e.V. (bwcon) ist die führende Wirtschaftsinitiative zur Förderung des Innovations- und Hightech-Standortes Baden-Württemberg. Als eines der größten Technologienetzwerke in Europa verbindet bwcon rund 600 Unternehmen und Forschungseinrichtungen. Mehr als 6.000 Mitglieder profitieren von der systematischen Vernetzung über die bwcon-Plattform. Darüber hinaus bietet bwcon ein umfangreiches Beratungs- und Betreuungsangebot sowohl für junge als auch expandierende Unternehmen an.

Ansprechpartner für die Presse
Nina Schulz
Baden-Württemberg: Connected e.V.
schulz@bwcon.de, Tel. 0711/90715-506