Mittelstand vernachlässigt Security – Forscher: „90 Prozent der Angriffe sind leicht abzuwehren"

Sicherheitslethargie bedroht die deutsche Volkswirtschaft

München (ab) – Eklatante Security-Schwächen im deutschen Mittelstand beklagt die Meta Group. Aber auch IT-Lieferanten sind gefordert.

„Nur fünf Prozent der mittelständischen Unternehmen hierzulande verhalten sich in Sachen IT-Sicherheit vorbildlich", schätzt Eduard Stupening, Senior Director Consulting bei der Meta Goup: „Security-Strategien sind Mangelware und fundierte Risikoanalysen die absolute Ausnahme." Auch seien bei Betrieben mit weniger als 500 Mitarbeitern keine Mehrausgaben für IT-Sicherheit geplant.

„Ein volkswirtschaftliches Risiko", mahnt Stupening, der dies für ein „sehr deutsches Problem" hält. Erstens gebe es hierzulande besonders viele kleine Betriebe, und zweitens sind etwa Briten viel aufgeschlossener gegenüber Security-Techniken. „Vielleicht sind wir Deutschen hier wie beim E-Government zu lethargisch", kommentiert Udo Helmbrecht, Chef des IT-Sicherheitsamts BSI.

Dass ordentlicher Schutz kein Hexenwerk ist, zeigt die Security-Tagung Dimwa. „90 Prozent der Angriffe können mit bekannten Maßnahmen verhindert werden", erläutert Ulrich Flegel von der Uni Dortmund – etwa durch Patch-Management und über eine Firewall, die leicht angreifbare Dienste wie Windows Netbios blockiert. Denn insbesondere Microsoft-Webserver sind Hackers liebstes Ziel. Und der Cyber-Untergrund schläft nicht: So verweist Flegel auf ein heuristisches Vergleichsverfahren für binären Programmcode, mit dem Angreifer – ohne den Sourcecode zu kennen – leicht nach strukturellen Unterschieden in gepatchten und ungepatchten Versionen suchen können, um Infos über das betroffene Sicherheitsloch gewinnen. Flegel: „Damit kann die Closed-Infopolitik vieler Hersteller Schaden anrichten, wenn ein Patch nur die Symptome unterdrückt, anstatt den Bug an der Wurzel zu packen."

Ein Beispiel: Microsoft stopfte jüngst nicht die grundlegende Lücke einer Windows-Bibliothek, sondern verwehrte über den Patch nur den Angriffsweg über eine bestimmte Anwendung – andere Applikationen blieben verwundbar. Und selbst die Java-Schiene ist nicht ohne Risiko, ergänzt Flegel: „Im Java Software Development Kit schlummern kritische Fehler, die Sun zwar bekannt, aber noch nicht behoben sind."

Überhaupt sei es Aufgabe der Hersteller, Sicherheit direkt in ihre Produkte einzubauen, so Meta-Mann Stupening, der „Security als Commodity" fordert. Dann kaufe der Mittelstand Sicherheit mit, ohne es zu merken. Auch BSI-Boss Helmbrecht sieht noch Defizite, etwa im Hause Microsoft. „Aber da haben wir mit unseren Opensource-Initiativen den Denkprozess schon beschleunigt."