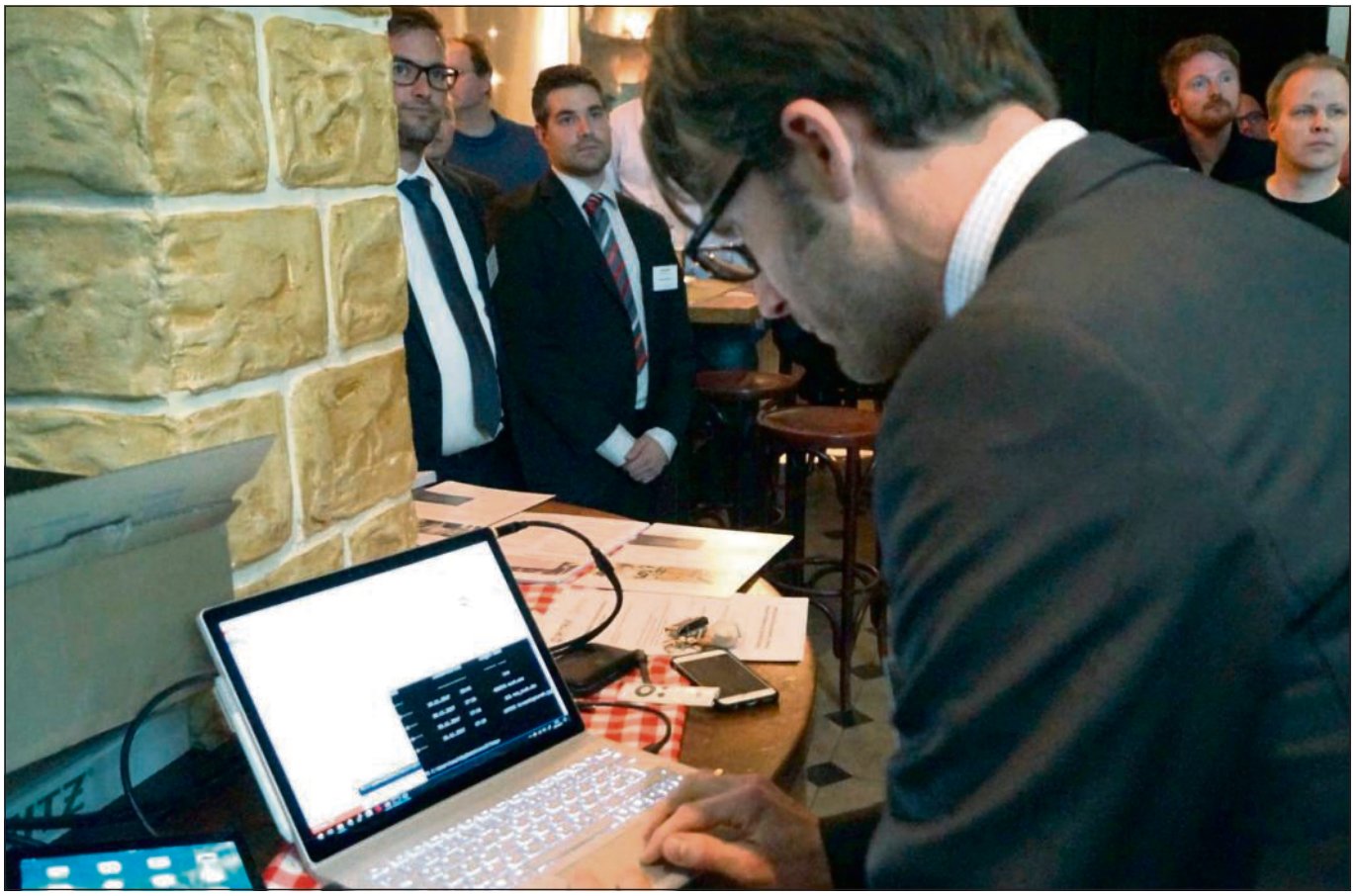

Einen USB-Stick gefunden und aus Neugier in den eigenen PC gesteckt – einfacher kann man es einem Hacker nicht machen, erklärte Max Ziegler und bewies beim Live Hacking wie schnell er an vertrauliche Daten und Screenshots kommen kann. ■ Foto: Klotz

Risikofaktor Mensch

Die Sicherheit von Unternehmen war Thema des ersten IT-Stammtisches

Von Jennifer Klotz

LIPPSTADT ■ „Das wohl schwächste Glied in der Kette der IT-Sicherheit ist der Mensch“, erklärte Professor Emanuel Slaby am Donnerstagabend beim ersten IT-Security-Stammtisch im Tivoli. Die Treffen könnten in loser Folge und ohne festes Programm fortgesetzt werden. Die Idee dazu hatte sich aus der Zusammenarbeit der IT-Security-Firmen Skytale und Carmao gebildet, denen sich das Projekt Mittelstand 4.0 angeschlossen hat. Unsere Redaktion hat den Abend, Fragen und Antworten verfolgt.

Warum spielt IT-Sicherheit eine immer größere Rolle?

Die Zahl der Cyber-Angriffe steigt stetig. So seien gut die Hälfte aller Unternehmen in Deutschland in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden, erklärte Max Ziegler, Akademieleiter bei Skytale.

Wie könnten Firmen dem entgegenwirken?

„Mit Unternehmensresilienz“, wusste Ulrich Heun (Carmao). Dieser aus dem Personalwesen entsprungene Begriff zur Krisenbewältigung durch Rückgriff auf vorher vermittelte Ressourcen ließe sich nämlich gut auf das ganze Unternehmen ausweiten. Das Ziel sei, die verschiedenen Fachbereiche durch Schulungen zusammenzubringen, damit diese gegen jegliche digitalen Angriffe gewappnet seien. Vorab solle eine Risikoanalyse durchgeführt werden – um Auswirkungen den Bereichen zuordnen und Maßnahmen ergreifen zu können. Wichtig sei auch die Schulung der Mitarbeiter.

Warum sind die Mitarbeiter ein Risikofaktor für die IT-Sicherheit – und was macht sie zum beliebten Ziel von Hackern?

„Zuerst einmal die Neugier“, zeigte Max Ziegler auf und hielt einen USB-Stick mit auffälligem Schlüsselanhänger hoch. „Eine Studie hat ergeben, dass rund 45 Prozent der gefundenen USB-Sticks in den eigenen PC gesteckt werden, um zu schauen, was da wohl drauf ist.“ Welche gravierenden Folgen das haben kann, demonstierte der Diplom-Informatiker per Live-Hacking direkt vor Ort.

Was passierte bei dem Live-Hacking?

Ziegler steckte den vermeintlichen USB-Stick in ein Zielgerät, wo er in Sekundenbruchteilen eine Verbindung zu seinem eigenen Rechner aufbaute. Diese bleibt auch bestehen, wenn der Stick den USB-Slot wieder verlässt. Ziegler: „Jetzt ist es schon zu spät. Der Hacker kann nun machen was er will, ohne dass Sie es merken.“ So konnte er ohne große Probleme unbemerkt Anwendungen starten, Screenshots und Webcam-Bilder machen oder sogar Daten übertragen.

Wie vorsichtig müssen Mitarbeiter sein?

Der irrigen Annahme vom klischeehaft aussehenden Hacker widersprach Emanuel Slaby, der an der Hochschule Hamm-Lippstadt „Informatik und Sicherheit in sozialen Medien“ lehrt. Denn Hacker, das könnte wohl auch der nette Postbote sein, der in großer Eile Firmenpakete abliefern will, von den Rauchern aus Mitleid reingelassen wird – und dann einen entsperrten PC sucht und den Stick einstöpselt. „Der Mensch ist leicht zu beeinflussen und will meistens helfen, wo er kann“, erläuterte der Professor. Das nutzten Hacker aus und könnten so sämtliche digitale Schutzmaßnahmen der Unternehmen umgehen.

Was ist mit den Passwörtern?

„13 Prozent der Menschen nutzen dasselbe Passwort für alle Dienste. Leichter kann man es den Hackern nicht machen“, mahnte Slaby. Er riet dazu, nicht nur verschiedene Passwörter, sondern auch Mailadressen zu nutzen. Das erschwere es Hackern ungemein.