Cyberschutz ist wichtig: *Die beiden Experten Torben Klagge und Jan Simon mit Eva Fischer, Heinfried Beermann und Sponsor Florian Hegemann (Allianz Generalvertretung Hegemann) sowie Christian Horlitz (Vorsitzender Wirtschaftsjunioren).* FOTO: SABINE GAUSEMEIER

Leichtes Spiel für Hacker

Cybersicherheit: Die Wirtschaftsjunioren Paderborn und Höxter machen sich schlau. Zwei Spezialisten präsentieren live, wie einfach der Datendiebstahl ist

■ **Paderborn**. Welche Risiken es birgt, mit dem Tablet gemütlich auf der Terrasse zu surfen, das erlebten die Teilnehmer des Themenabends „Cybersicherheit", zu dem der Arbeitskreis Marketing der Wirtschaftsjunioren Paderborn und Höxter eingeladen hatte.

In der Paderborner Garage 33 im Technologiepark Paderborn zeigten unter anderem zwei Spezialisten für IT-Sicherheit bei einem spannenden Live-Hacking, wie verblüffend einfach es ist, Daten zu sammeln und Schadsoftware einzuschleusen – ohne dass der Nutzer es merkt.

Mit verteilten Rollen führten „Täter" Torben Klagge und „Opfer" Jan Simon von der Hamburger IT Sicherheitsberatung Sopra Steria Consulting durch den Arbeitstag eines Geschäftsführers. Und der setzt sich morgens vor der Arbeit gerne mal auf die Terrasse, um per Tablet Nachrichten zu lesen und seine E-Mails abzurufen. „Anhand der gespeicherten WLAN-Liste wählt Ihr Mobilgerät automatisch das Netz mit dem stärksten Signal", sagte Klagge. Für einen Angreifer sei es also leicht, Gewohnheiten auszuspähen, selbst ein Netzwerk mit einem geläufigen Namen einzurichten und aus 50 Metern Entfernung ein so starkes Signal zu senden, dass sich das Tablet dort einwählt.

Als dazwischengeschalteter „Man-in-the-Middle" komme der Angreifer dann nicht nur an Informationen, sondern auch an sogenannte Session-IDs. „Damit wiederum kann ich einem System vortäuschen, ein valider anderer Nutzer zu sein und zum Beispiel in dessen Namen unbemerkt in das Unternehmensnetzwerk gelangen", erläutert Klagge und führte den erstaunten Zuschauern vor, wie leicht sich so Preise oder Gehaltslisten manipulieren lassen. „Löschen Sie also regelmäßig die öffentlichen Netzwerke in Ihrer WLAN-Liste."

Gefährlich seien auch die von Hackern programmierten und im Darknet erhältlichen „Exploits". „Diese kleinen Stücke Schadsoftware nutzen bestimmte Schwachstellen von Programmen aus", erklärte Klagge. „Doch dazu müssen sie zunächst einmal irgendwie auf Ihren Rechner kommen." Das geschehe meist in Form einer getarnten Datei, zum Beispiel als E-Mail-Anhang oder Mediaplayer-Datei.

„Öffnen Sie niemals Dateien unbekannter Herkunft, auch keine PDFs." Zwar böten Virenscanner und Patches im Wettlauf mit den Hackern einen recht guten Schutz, „wenn der Virus jedoch auf sein spezielles Opfer zugeschnitten ist, hilft Ihnen das meist nicht".

Auch das „Phishing" per E-Mail mit Links zu gefälschten Webseiten sei heutzutage exzellent gemacht, warnte der Sicherheitsprofi. „Beachten Sie unbedingt, dass der vertrauenswürdig wirkende hinterlegte Link nicht der tatsächlichen Webadresse entsprechen muss." Es gebe auch sehr gezielte Formen, wie falsche Mails, in denen geänderte Bankdaten von Dienstleistern übermittelt werden oder die Mail vom Chef, der anordnet, Geld zu überweisen. „Die meisten Menschen halten E-Mails für sicher und vertrauenswürdig", so Klagges Erfahrung. „Sind sie aber nicht. Fragen Sie im Zweifel gerade bei kritischen Vorgängen möglichst persönlich nach."

Auch beim Drumherum müssen IT-Nutzer wachsam sein. „Eine geschenkte Maus zum Bespiel kann Schadsoftware installieren, öffentliche USB-Ladestationen ebenfalls", warnte Klagge.