



Nobody is perfect

„Social Engineering“ bedeutet, Menschen zu beeinflussen, um illegal an Daten oder Dinge zu gelangen. Ansatzpunkt sind dabei häufig Schwächen wie Bequemlichkeit oder Unachtsamkeit. Für die IT-Sicherheit nutzen daher die besten technischen Vorkehrungen wenig, wenn der „Faktor Mensch“ vernachlässigt wird.

Cyberkriminelle setzen auf eine Vielzahl an Betrugsmethoden, um die Computer von Anwendern zu kapern und illegal Geld zu verdienen. Dabei bedienen sie sich ausgeklügelter Techniken, um Malware-Aktivitäten zu verbergen oder den Antiviren-Experten das Auffinden, Erkennen und Analysieren von Schadcode zu erschweren. Das Phänomen Cyberkriminalität unter rein technischen Aspekten zu betrachten, liegt daher nahe. Aber: „Wenn man Cyberkriminalität und Lösungen dagegen erörtern will, ist es unerlässlich, auch den ‚Faktor Mensch‘ mit einzubeziehen“, sagt David Emm, Senior Security Researcher bei Kaspersky Lab.

Hintergrund: Trotz der technischen Raffinesse moderner Schadprogramme versuchen Cyberkriminelle häufig, menschliche Schwächen wie Bequemlichkeit, Unachtsamkeit oder auch Gier auszunutzen, um ihre Schädlinge zu verbreiten. Kein Wunder, denn der Mensch ist oft das schwächste Glied in einem Sicherheitssystem. Ein Beweis dafür sei nach Meinung des Experten der anhaltend große Erfolg von Phishing-Betrügereien, mit denen Anwender dazu gebracht werden sollen, persönliche Daten wie Benutzernamen, Passwörter oder PINs, die für Cyberkriminelle von Nutzen sein könnten, auf gefälschten Webseiten einzugeben. Der klassische Phishing-Betrug wird mittels einer nachgeahmten E-Mail initiiert, die an Millionen von E-Mail-Adressen gespart wird, in der Hoffnung, dass genügend Leute auf den Betrug hereinfliegen und auf den in der Spam-Mail enthaltenen Link klicken. „Derartige Attacken sind nach wie vor beliebt und für Online-Kriminelle immer noch höchst erträglich“, sagt Emm.

PASSWORT-DURCHEINANDER

Daneben birgt die Bequemlichkeit vieler Menschen ein hohes Gefährdungspotenzial, gerade was den Gebrauch von Passwörtern angeht. Das Problem dabei: Immer mehr Alltagsgeschäfte werden online abgewickelt – einkaufen, Bankgeschäfte, das Bezahlen von Rechnungen, professionelles Networking etc. Heute ist es nichts Besonderes mehr, wenn man zwischen zehn und dreißig Online-Accounts nutzt. Die Folge: Es wird immer

schwieriger, für jeden einzelnen Account ein individuelles Passwort im Kopf zu behalten.

Die Versuchung ist also groß, ein und dasselbe Kennwort für alle Accounts zu benutzen oder den Namen eines Kindes oder des Ehepartners zu wählen. Eine andere gängige Methode ist das „Recyclen“ von Passwörtern, indem man ein und dasselbe Passwort zum Beispiel aufsteigend durchnummeriert („meinname1“, „meinname2“, „meinname3“). Passwörter sind daher oft leicht zu knacken. Die Wahrscheinlichkeit, dass Cyberkriminelle relativ problemlos Zugang zu Internet-Accounts erhalten, ist hoch. Dieses Risiko wird von vielen Anwendern allerdings immer noch häufig unterschätzt. Was also ist zu tun? „Der Königsweg zu einer wirklich ausreichenden Sicherheitsstrategie besteht darin, menschliche Sicherheitslücken zu schließen und digitale Ressourcen zu schützen“, erklärt Emm.

Dabei sei es zunächst einmal wichtig, Erziehung nicht mit Ausbildung zu verwechseln. „Es wäre unrealistisch, die breite Masse zu Computer-Sicherheitsexperten ausbilden zu wollen. Wir sollten vielmehr das Bewusstsein für potenzielle Online-Bedrohungen stärken und Maßnahmen vermitteln, mit denen sich Anwender selbst schützen können.“ Für Unternehmen und Organisationen sollte die Erziehung der Mitarbeiter allerdings das Herzstück jeder effektiven Sicherheitsstrategie sein.

Dabei sollten den Mitarbeitern Bedrohungen in einfacher, klarer Sprache erklärt wer-

den, sodass sie nachvollziehen können, welche Schutzmaßnahmen das Unternehmen warum eingeführt hat und welche Auswirkungen diese in ihrer täglichen Arbeit haben können. Denn nach Meinung Emms sei eine Sicherheitsstrategie weitaus effektiver, wenn das Personal sie versteht und unterstützt. Zudem empfiehlt er Unternehmen, eine Kultur der Offenheit zu etablieren: Diese soll die Mitarbeiter ermutigen, verdächtige Aktivitäten zu melden, statt diese aus Angst vor disziplinarischen Folgen zu verheimlichen.

Es reicht nicht, eine Sicherheits-Policy zu entwickeln, diese dann von den Mitarbeitern unterzeichnen zu lassen und darüber hinaus nichts zu unternehmen. Eine effektive Sicherheitsstrategie sollte der sich verändernden Bedrohungslandschaft angepasst sein und deshalb regelmäßig überprüft werden. Dabei sollte man auch bedenken, dass jeder einzelne Mitarbeiter auf unterschiedliche Weise lernt: Der eine reagiert besonders gut auf mündlichen Input, der andere auf schriftliches oder illustriertes Material. Daher sollten verschiedene Strategien angewendet werden, um das allgemeine Sicherheitsbewusstsein zu schärfen. Das schließt Präsentationen als Teil der Mitarbeiterschulung ebenso mit ein wie Posterkampagnen, Ratespiele, Comics und einen „Tipp des Tages“, der beispielsweise angezeigt wird, wenn sich ein Mitarbeiter ins Unternehmensnetzwerk einloggt.

Wichtig ist nach Meinung des IT-Sicherheitsexperten zudem, dass man Sicherheitsschulungen und -informationen nicht nur unter dem IT-Aspekt sieht. Das Thema sollte vielmehr im großen Kontext der Personalpolitik eingebunden werden, der Bereiche wie Arbeitssicherheit und -gesundheit ebenso wie richtiges Verhalten am Arbeitsplatz miteinschließt. „Ein wirklich effektives Sicherheits-erziehungsprogramm muss Anleihen aus der Personalabteilung, der Schulungsabteilung und allen anderen relevanten Unternehmensbereichen vorweisen.“

BERUF UND PRIVAT

Ein weiterer zu berücksichtigender Aspekt: Beim Einsatz von Computern zu Hause und bei der Arbeit gibt es Überschneidungen. Anwender, die den PC als Arbeitsgerät im Unternehmen nutzen, verwenden ihn auch, um von zu Hause aus einzukaufen, Bankgeschäfte zu erledigen und Kontakte zu pflegen. Daher empfiehlt Emm, die Verwendung des Computers zu Nichtarbeitszwecken in das Sicherheitstraining des Personals mit einzubinden: „Zeigt man den Mitarbeitern, wie sie ihren eigenen Computer schützen und ihren eigenen Router sichern können, steigt die Motivation, am Sicherheitstrainingsprogramm aktiv mitzuwirken und es zu unterstützen.“ Damit lasse sich auch die Gefährdung von Unternehmensressourcen durch Mitarbeiter, die heute immer häufiger von zu Hause aus arbeiten, minimieren.

Zwar sind sowohl Gesetzgebung als auch Initiativen zur Durchsetzung der Gesetze darauf ausgelegt, das Risiko für die Cyberkriminellen zu maximieren. Der Sinn und Zweck von Technologien und Erziehungsstrategien liegt darin, das Risiko für die Gesellschaft zu minimieren. Da viele der Cyberattacken heute auf die Fehlbarkeit des Menschen abzielen, ist es unumgänglich, nach Wegen zu suchen, die die Schwachstelle Mensch mitberücksichtigen – ebenso wie die Sicherung von Hard- und Software. „Mit der Sicherheitserziehung verhält es sich wie mit der täglichen Hausarbeit“, bilanziert Emm. „Mit der einmaligen Erledigung ist es nicht getan, man muss sich ständig darum kümmern, wenn man seine Umgebung sauber und sicher halten möchte.“ (dam) ■



KOPFZERBRECHEN: Der menschliche Faktor ist und bleibt eine große Schwachstelle in der IT-Sicherheitskette. Sicherheitsschulungen und -informationen sind deshalb für eine effektive Sicherheitsstrategie unverzichtbar.