

Per Mausklick in fremde Computer

Ein „Profi-Hacker“ zeigt, wie schnell Konten und Passwörter geknackt sind

Passwörter knacken? In Minutenschnelle. Online-shops manipulieren? Eine Fingerübung. Vor rund 150 Gästen verschafft sich „Profi-Hacker“ Daniel Schalberger im Nino-Hochbau Zugang zu Computern und Datenbanken. Dabei zeigt er auf, mit welchen Tricks Kriminelle im Internet arbeiten.

Von Norman Mummert

NORDHORN. Wie eine Seifenblase hat Daniel Schalberger das Gefühl von Sicherheit und Schutz im Internet platzen lassen. Die Wirtschaftsförderung des Landkreises, die Grafschafter Volksbank und der Marketingverein Nino-Hochbau hatten den „Profi-Hacker“ aus Tübingen eingeladen, auf der Bühne im Manz-Saal anschaulich zu zeigen, wie schnell Passwörter geknackt und die Kontrolle über fremde Computer erlangt werden kann.

Scheinbar mühelos lässt er die Finger über die Tastatur seiner aufgestellten Laptops fliegen und bringt Internetseiten mit kurzen Computerbefehlen dazu, ganze Listen und Datenbanken mit Nutzerinformationen preiszugeben. Darunter befinden sich neben Nutzernamen auch die Passwörter.

Die Betreiber der Internetseite haben durchaus Vorkehrungen getroffen und die Kennwörter verschleiert. Sie erscheinen als eine auf den ersten Blick unzusammenhängend wirkende Ansammlung von Zahlen und Buchstaben – als sogenannte Streuwertfunktion, im Fachjargon „Hash“ (englisch für zerhacken) genannt. Einmal in eine Streuwertfunktion umgewandelt, lässt sich diese mathematische Funktion nicht mehr zurückrechnen. Das Passwort scheint ge-



In Minutenschnelle knackt er Passwörter und hackt sich in fremde Systeme ein: Daniel Schalberger, Hacker und IT-Sicherheitsberater der Firma Syss aus Tübingen, zeigt auf, wie verwundbar Nutzer im Internet sind. Foto: Westdörp

schützt. Ein Trugschluss: Der gewiefte Hacker kennt Programme, die selbst verschleierte Kennwörter entschlüsseln – und somit für ihn nutzbar machen.

Sind etwa E-Mail-Adresse und Passwort herausgefunden

– ANZEIGE –
www.malermeister-bült.de

den, liegt es für den Hacker nahe, diese auch in sozialen Netzwerken wie Facebook auszuprobieren, erklärt Schalberger. Oft würden Nutzer dieselben Kennwörter für verschiedene Konten nutzen. Oder für den Hacker noch interessanter ist die Frage: Hat der Nutzer beispielsweise eine Fernschaltung auf einen Firmencomputer, mit dem er von zuhause aus arbeitet? Und verwendet er dort dieselben Anmeldedaten? Dann kann er dort

unter Umständen auf das firmeninterne Netzwerk zugreifen und große, wirtschaftliche Schäden anrichten.

Konkrete Beispiele hat Hubert Lanzerath von der R+V Versicherung im Gepäck. Er berichtet von Hackern, die im Namen eines tschechischen Energieversorgers Kupferrohre bestellt hatten. Diese wurden hergestellt und geliefert. Der tatsächliche Energieversorger bekam im Anschluss die Rechnung, wies diese aber zurück, denn er hatte die Rohre weder gekauft noch erhalten. Der Kupferrohrhersteller verlor rund 100 000 Euro, berichtet Lanzerath.

In einem weiteren Beispiel hatten sich Hacker in das Telefon eines Betriebs eingeschlichen und am Wochenende mehrmals eine Nummer in Aserbaidschan angerufen. Die Telefonkosten waren „immens“, sagt Lanzerath.

„Wir kommen heute ohne

Internet, EDV und mobile Kommunikation nicht mehr aus“, sagt er. Die einzige Sicherheit biete, alle Verbindungen zum Internet zu kapfen. „Aber dann kann man nicht mehr arbeiten“, resümiert er. „Wir müssen damit leben, dass wir angegriffen

– ANZEIGE –
Blasinstrumente
Musik Fockers
www.musik-fockers.de, Tel. 05971 800150

werden. Netzsicherheit gibt es nicht. Die Frage ist, wie wir uns verteidigen.“

Als Fachmann für Schwachstellen in Computern und auf Webseiten hat Daniel Schalberger einige Tipps parat:

- Obwohl es einen 100-prozentigen Schutz im World Wide Web nicht gibt, rät Schalberger zu **Virenschernern**. „Damit können 98 Prozent der Angriffe abgewehrt werden“, erklärt er.

- Um die Daten auf dem

Computer zu sichern, sollten regelmäßig sogenannte **Backups** angelegt werden.

- Programme sollten **regelmäßig aktualisiert** werden. Hacker können sonst Programmierfehler ausnutzen und somit auf den Computer zugreifen.

- Es sollten möglichst **lange Passwörter** gewählt werden, die aus mindestens zehn Zeichen bestehen. „Ein Kennwort mit acht Zeichen knackt ein Hacker an einem Wochenende“, sagt Schalberger. Neun Zeichen schaffe ein Hacker in einer Woche. „15 Zeichen schafft er nicht mehr in diesem Leben.“

- Für Konten auf verschiedenen Internetseiten sollten **unterschiedliche Passwörter** benutzt werden.

- Das Knacken einer Streuwertfunktion kann zusätzlich erschwert werden, indem Nutzer etwa Begriffe und Sätze verwenden, die nicht in Wörterbüchern zu finden sind. Als Beispiel nennt Schalberger: „Das Nilpferd trinkt grüne Tinte“.

- Die größte Gefahrenquelle für Mobilfunkgeräte wie Smartphone oder Tablet-PC sind **Applikationen**, erläutert Schalberger. Daher empfiehlt der Experte, sie nur in offiziellen Online-Shops herunterzuladen.

„Das ist existenzbedrohend“, fasst Ralf Hilmes von der Wirtschaftsförderung des Landkreises die Präsentation Schalbergers und den Vortrag Lanzeraths zusammen. „Die Welt befindet sich auf Digitalisierungskurs. Was digitalisiert werden kann, wird digitalisiert. Und was heute noch nicht digitalisiert werden kann, ist morgen möglich.“

Die Veranstaltung habe ihn „nachdenklich und sensibel“ gestimmt. Deshalb appelliert er an die Unternehmer unter den rund 150 Gästen: „Machen Sie IT-Sicherheit zur Chefsache!“