Aus dem Blickwinkel der Sicherheitsexperten:

MÄCHTIGE HACKER-WERKZEUGE

From the point of view of security experts: powerful hacking tools

Die „gläsernen“ Mitarbeiter – so bereiten Hacker ihre Angriffe vor

Wer ist wer in Ihrem Unternehmen? Wer kennt wen? Wie baut ein Hacker Vertrauen bei den für ihn entscheidenden Mitarbeitern auf und benützt sie dann als seine Marionetten? Sehr einfach: man findet vorab alles über sie heraus.

Als Handy-Nutzer und facebook-Freunde hinterlassen wir alle eine tägliche Datenspur im Netz. Die Tools zur Analyse und Verknüpfung solcher Daten stehen für jedermann kostenlos im Netz. Sie wurden über Jahre weiterentwickelt und werden von Strafverfolgungsbehörden und Geheimdiensten benützt. Eine große User-Gruppe daneben: Hacker in der Vorbereitung ihrer Angriffe.

Ein weit verbreitetes Werkzeug ist das Informationsbeschaffungs- und Visualisierungstool „Maltego“. Mit ihm werden aus E-Mail- und Netzwerk-Adressen Rückschlüsse über persönliche und berufliche Informationen, soziale Netze, Zusammenhänge und Verhaltensweisen gezogen.

Das Programm arbeitet sich sukzessive durch Datenberge durch und bereitet die Schlüsse in schönen Grafiken auf. Die Analysefähigkeiten legen soziale Beziehungen von Menschen offen, von denen man ursprünglich nicht mehr wusste als deren Namen.

Funktioniert das nur bei „heavy internet usern“?

Wir googlen die neuesten Wirtschaftsdaten, recherchieren zu potentiellen Kunden und neuen Märkten oder möglichen Wettbewerberangeboten. Nebenher schauen wir das lustige Video, das die Kollegen gefunden haben, stöbern in den neuesten Angeboten beim Supermarkt um die Ecke oder suchen Möglichkeiten, unser Geld anzulegen. Google & Co sind die Lexika für nahezu alles, was uns jetzt in dieser Minute interessiert.

Wir kommunizieren per E-Mail, empfangen Newsletter, schicken Anfragen an andere Unternehmen, nutzen Skype, Chat, Instant Messaging und Online Banking. Die größten Identitätsdatenbanken der Welt – facebook und Co – kennen sowieso unseren Realnamen, die Schule, die Uni, unsere „Likes“, unseren Schreibstil. Die Fotosammlung, die mit Gesichtserkennung ausgelesen wird, verlinken wir in sozialen Medien mit den Profilen von Kollegen und Freunden, und selbst wenn wir das nicht tun, sammeln die Netzwerke Daten über uns. Weil einige Fotos so schön sind, nutzen wir sie auch in pseudonymen Profilen. Und da ist ja noch das Foto der Abschlussklasse, das Teamfoto des Arbeitgebers auf LinkedIn, der Kurz-CV mit meinen Gehaltsvorstellungen für interessierte Arbeitgeber auf LinkedIn. Und wo ich gerade bin, lässt sich anhand der Position eines Rechners oder – noch exakter – mithilfe der GPS-Sensoren in Smartphones ermitteln. Glauben Sie immer noch nicht, dass man mit ihrer Emailadresse viel anstellen kann?

“Transparent” employees – this is how hackers prepare for their attacks

Who is who in your company? Who knows whom? How can hackers win the trust of employees that are of decisive significance for them, so that they can use them as their tools? As easy as pie: by finding out everything about them in advance.

As mobile phone or facebook users, we leave data traces on the web every day. The tools for analysing and linking such data are available for anyone on the Internet. They have been refined for years and are being used by law enforcement authorities and intelligence agencies. Another large group of users: hackers preparing for their attacks.

A commonly used tool is Maltego, a data mining and visualisation tool. It can be used to draw conclusions from e-mail and network addresses regarding personal and professional information, social networks, relationships and behaviour.
The software gradually processes huge amounts of data and presents the conclusions in neatly arranged graphs. These analyses allow to expose the social relationships of individuals of whom originally nothing but their name was known.

Does this work for “heavy internet users” only?

We google the latest business data, we do research on potential customers and new markets or potential products offered by competitors. In between, we watch the funny video found by our colleagues, we browse through the most recent bargains in the supermarket around the corner or look for ways to invest our money. We use Google and the like as encyclopedias for nearly everything we want to look up right this minute.

We communicate via e-mail, receive newsletters, send enquiries to other companies, we use Skype, chats, instant messaging and online banking. The largest identity databases in the world – such as facebook – know our real names, our school, our university, our “likes”, our style of writing. We link the photo collection (that is read using facial recognition) in social media to the profiles of colleagues and friends, and even if we don’t – the networks are collecting data about us. We also use some of our best pics for pseudonymous profiles. Then there is the photo of the final-year class, the team photo of the employer on LinkedIn, the brief CV with my salary requirement for potential employers on LinkedIn. The position of my computer or – even more accurate – the GPS sensors in my smartphone reveal where I am at this precise moment. Do you still refuse to believe that your e-mail address can be (mis)used for a lot of things?