9311 Punkte
+0.66%

Gewinner		Verlierer	
ɔcean N	+3.42%	Julius Bär N	-0.19%
lecco N	+1.58%	Roche GS	-0.04%
olcim N	+1.42%	Actelion N	0.00%

es Ind. 18054 Punkte
+0.42%

xx 3607 Punkte
+0.47%

anken	1.042	-0.41%
Franken	0.945	-0.35%
ollar	1.102	-0.06%
d in Franken	1.473	-0.07%
ee Brent) in Dollar	57.43	-0.47%
e) in Dollar	1155.70	0.33%
nze) in Dollar	15.36	-0.10%

richten

ort

-Verbände wehren sich n Buchungszuschläge

eise-Verbände der Schweiz, hlands und Österreichs wehren egen die von der Lufthansa- e geplanten Buchungszuschläge. iftfahrtkonzern solle auf den ab ber geplanten Aufschlag von ken pro Buchung über das glo- eservierungssystem (GDS) ver- . Die Lufthansa-Gruppe und die treiber müssten gemeinsam eine g für ihre Kosten- und Ent- ktur finden, heisst es in einem uniqué der drei Branchenorgani- en Schweizer Reise-Verband Deutscher Reiseverband (DRV) Österreichischer Reiseverband om Dienstag. *(SDA)*

rie

rlikon reagiert auf chte um Vakuum-Verkauf

lustriekonzern OC Oerlikon prüft gische Optionen» für das Seg- akuum, wie er am Dienstagabend e. Zum gegenwärtigen Zeitpunkt doch zu früh, um konkrete Aus- u machen. Mit der Mitteilung rea- Oerlikon auf Gerüchte zu einem en Verkauf des Geschäfts mit Va- umpen. Die Nachrichtenagentur s hatte am Dienstag mit Berufung der berichtet, das Unternehmen ie Deutsche Bank mit der Suche nem Käufer beauftragt. Der Ge- bereich, der Vakuumtechnologie lschränke oder die Beschichtung ikrochips liefert, könnte laut s bei einer Veräusserung mit 350 0 Millionen Franken bewertet . *(SDA)*

ht über Übernahme e für Aufregung

enbar gefälschter Medienbericht ne Übernahme des US-Kurznach- diensts Twitter hat gestern an rkten für viel Aufregung gesorgt. itter-Aktie sprang an der Wall- eitweilig bis zu acht Prozent in e. In dem Bericht auf einer Inter- die zunächst fälschlicherweise entur Bloomberg zugeordnet hiess es, dass Twitter für 31 Mil- Dollar übernommen werden as Unternehmen arbeite deshalb mit Banken an einer entspre- n Strategie. Wenig später stellte cher der US-Agentur jedoch klar, Bericht eine Fälschung sei. Auch wies den Bericht über eine an- e Offerte zurück. Im April hatte es tionen gegeben, dass der Inter- ern Google eine Übernahme von erwäge. *(Reuters)*

Tages-Anzeiger 15.7.15

Bitte brechen Sie bei uns ein!

Ivano Somaini verschafft sich Zugang zu Banken, um deren Sicherheitssysteme zu testen. Seine Werkzeuge: Gefälschte E-Mails, hilfsbereite Angestellte und teils ausgefallene Verkleidungen.

Mario Stäuble

«Irgendwo findet man immer eine Lücke», sagt ETH-Informatiker Ivano Somaini. Foto: Urs Jaudas

Ivano Somaini liebt die Schauspielerei seit seiner Jugend – aber auf diese Rolle hat ihn niemand vorbereitet. Schwitzend steht er vor der Einfahrt zur Tiefgarage einer Zürcher Privatbank, in einen Anzug gekleidet, eine Kartonschachtel in den Händen, gefüllt mit Büchern und Krimskrams. Er rechnet damit, dass sich das Tor zwischen 7 und 7.30 Uhr mindestens einmal öffnen wird, um einen Lieferdienst passieren zu lassen, der die hausinternen Kaffeemaschinen auffüllen würde. Er weiss das, weil er den Tag zuvor wartend vor dem Gebäude verbracht hat. Er weiss auch, dass es 16 bis 17 Sekunden dauern wird, bis der Schliessmechanismus wieder einrastet. Reichlich Zeit, um hinter dem Lieferanten in die Garage zu schlüpfen.

Der Auftrag lautet: Dringe in den inneren Bereich des Gebäudes ein und fotografiere vertrauliche Dokumente oder USB-Sticks, die du stehlen könntest.

Kurz nach 7 Uhr taucht in der Tat das Kaffeefahrzeug auf. Somaini eilt dem Wagen hinterher, die Einfahrt hinunter, über die Schwelle der Garage. Hinter ihm schliesst sich das Tor.

Das nächste Problem ist der Eingang ins Kellergeschoss der Bank. Zutritt nur mit Badge. Somaini begibt sich in Hörweite der Kaffeelieferantin, die gerade aus dem Auto steigt, klaubt sein Mobiltelefon aus der Tasche und täuscht ein hektisches Gespräch vor: «Ja, ja ich bin hier. Ja, ich bin zu spät dran. Ich komme gleich in den vierten Stock.» Als die Frau in Richtung Tür losgeht, folgt Somaini ihr. Nahezu gleichzeitig kommen die beiden am Badgeleser an. Die Lieferantin glaubt einen jungen Banker zu erblicken, der in Eile und schwer beladen ist. Ohne dass weitere Worte nötig gewesen wären, öffnet sie ihm mit ihrer Karte das elektronische Schloss. Er ist drin.

Nun spürt Somaini das Adrenalin – er muss sich beruhigen, bevor er den Lift in die oberen Stockwerke betritt. Also versteckt er sich in einer Toilette und ruft seine Mutter an. Zehn Minuten plaudert er über Geschwister und Grosseltern, während sich seine Herzfrequenz langsam senkt.

Menschen hacken

So habe sein erster «Einbruch» angefangen, erzählt Ivano Somaini heute. Der 31-Jährige arbeitet seit 2011 bei der Sicherheitsfirma Compass Security in Bern und Jona SG. Das IT-Unternehmen macht seinen Umsatz unter anderem mit «Penetration Testing». Das bedeutet: Die Techniker attackieren die Systeme von Banken, Energiekonzernen, Militär oder Regierung, um zu prüfen, ob sich darin Lücken finden lassen, die böswillige Hacker ausnutzen könnten. Banken bestellen etwa solche «Pentests», bevor sie eine neue E-Finance-Plattform für ihre Kunden aufschalten. In der Schweiz gibt es inzwischen einige Dutzend Firmen, die in diesem Bereich tätig sind.

Manche dieser Unternehmen gehen einen Schritt weiter. Sie hacken nicht nur Programme, sondern auch Menschen. «Social Engineering» nennt sich das, «soziales Manipulieren». Es gehe darum, den Leuten eine Geschichte in den Kopf zu pflanzen und das auszunutzen, sagt Somaini. Die Werkzeuge: falsche Nachrichten, Anrufe, Verkleidungen, Lügen. Das Ziel ist dasselbe: Schwächen in Sicherheitssystemen aufdecken. Menschliche Schwächen.

Darauf hat sich Somaini spezialisiert. Der ETH-Informatiker, aufgewachsen im italienischsprachigen Teil Graubündens, sprach «sehr, sehr, sehr schlecht Deutsch», als er in Chur ins Gymnasium kam. Um Anschluss zu finden, meldete er sich bei einer Theatergruppe an, «lauter Steinbock-Tschinggelis wie ich». Seither fasziniert ihn das Spiel mit der eigenen Identität. An der ETH konzentrierte er sich auf Sicherheit und Kryptografie (der Vater ist Kirchenrestaurator, von ihm habe er die Faszination für Rätsel und Muster). Nach dem Masterabschluss googelte er «Penetration Tester, Schweiz». Und kam bei Compass Security unter.

Heute leitet er dort ein Team von Technikern, mit dem er ein Dutzend Social-Engineering-Aufträge erledigt hat. Seine Leute sind schon als Elektriker, Lüftungstechniker, Banker oder Studenten aufgetreten, um Rezeptionisten und Wachleute in die Irre zu führen.

Als Samichlaus verkleidet

Einmal, an einem 6. Dezember, versuchte Somaini es als Samichlaus. Er wurde vom Empfangsdesk ohne Kontrolle durchgewinkt, weil die Firma tatsächlich einen Chlaus gebucht hatte. So kam er in den gesicherten Bereich, zog

> «Die Leute sollen denken: Mein Gott, das hätte auch ich sein können, der ihm die Tür aufhielt.»
> Ivano Somaini, Penetration Tester

einen Anzug an, den er im Gabensack versteckt hatte – und konnte sich frei im Gebäude bewegen. «Am besten funktionieren Angriffe, welche die Instinkte der Leute ausnutzen.» Hilfsbereitschaft, Angst, Neugier.

In einem Fall richtete er ein E-Mail-Konto ein, das dem Namen eines Bankkaders glich, von dessen Geldhaus er einen Auftrag erhalten hatte. Unter dieser Identität verschickte er eine kurze Nachricht:

«Lieber XY, hier noch die aktuelle Bonuskalkulation.»

Das E-Mail ging an die gesamte Belegschaft der Bank. «Es sollte so aussehen, als ob die Nachricht eines Kadermanns an einen anderen Kadermann versehentlich ‹an alle› gegangen war», sagt Somaini. Angehängt war ein Excel-File mit dem Titel «Bonus-Rechner». Tatsächlich steckte in der Datei ein Wurm, der sich selbst aktivierte, sobald man sie öffnete. Zwei Drittel der Angestellten konnten nicht widerstehen und klickten.

Der freundliche Fremde

Meist folgen nach einem Angriff Analysen und Schulungen im Unternehmen, in den Somaini Risiken identifiziert: Der freundliche Fremde im Flur. Das E-Mail, das zu gut klingt, um wahr zu sein. Der USB-Stick, der als Geschenk mit der Post kam. Man finde immer irgendwo eine Lücke, sagt Somaini. Der Sinn der Tests liege vor allem darin, einen Lerneffekt hervorzurufen: «Die Leute sollen denken: Mein Gott, das hätte auch ich sein können, der ihm die Tür aufhielt.» Manchmal soll dieser Effekt ganz oben in der Hierarchie eintreten. Etwa wenn der Sicherheitschef das löchrige System prüfen lässt, um der Geschäftsleitung deutlich zu machen, dass man das Security-Budget aufstocken sollte.

Nicht dafür da, zu bestrafen

Und manchmal werden zweifelhafte Ziele verfolgt: Ein Kadermann wollte in einem Fall einen unliebsamen Mitarbeiter testen lassen, um ihm dann Versagen vorzuwerfen und damit die Kündigung begründen zu können. «Solche Aufträge machen wir nicht», sagt Somaini. Allgemein rät er Kunden davon ab, Mitarbeiter zu bestrafen, die «Opfer» eines Tests geworden sind.

Für die Angreifer selbst ist der Job nicht ohne Risiko. Sollte ein Versuch schiefgehen, ist schnell die Polizei im Spiel. Deshalb tragen die falschen Einbrecher einen Brief des Sicherheitschefs auf sich, der bestätigt, dass die Attacke bewilligt ist. Gebraucht hat Ivano Somaini diesen Freibrief noch nie.

Auch in der Zürcher Privatbank nicht. Dort nimmt er den Lift nach oben, nachdem er die Männertoilette verlassen hat. Es gilt nun, vom äusseren in den inneren Sicherheitsbereich des Gebäudes zu kommen. Das ist nicht mehr ganz so schwer: Wer ihn sieht, geht davon aus, er sei bereits am Eingang kontrolliert worden.

Vor der Tür der Personalabteilung tätigt er erneut einen Fakeanruf, um den Eindruck zu erwecken, jemand erwarte ihn drinnen zu einer Sitzung. Und erneut öffnet ihm ein hilfsbereiter Angestellter die elektronisch verschlossene Tür. Somaini betritt die Abteilung, findet ein leeres Büro und fotografiert die Dokumente, die auf dem Schreibtisch liegen.

Auftrag erledigt, Bank geknackt.

Wie man sich schützt
Die wichtigsten Tipps

Bei merkwürdigen Aufträgen per SMS oder Mails: Adresse des Absenders überprüfen, auf anderem Kanal nachfragen. Ein Smartphone ist genauso auf Angriffe empfindlich wie ein Computer.

- Bei Mails: Keine Attachments anklicken, wenn der Absender unbekannt ist. Besondere Vorsicht bei ausführbaren Dateien.
- Wenn der Abwesenheitsassistent aktiviert ist: Signatur weglassen, um zu verhindern, dass Kontaktdaten automatisch an neugierige Nachrichtenschreiber gesendet werden.
- In sozialen Netzwerken: Die Einstellungen zur Privatsphäre gegenüber Fremden restriktiv festlegen.
- USB-Sticks, deren Herkunft man nicht kennt, nicht verwenden.

Bilder Tipps gegen Social-Engineering-Angriffe

somaini.tagesanzeiger.ch