Zug um Zug

Fragwürdiger Entscheid

Die rund 800 Meter lange Busspur an der Chamerstrasse mitbenutzen zu dürfen, das beantragte der Verein Tixi Zug beim Regierungsrat. Dies, weil es aufgrund der Verkehrslage für den Fahrdienst für Menschen mit Behinderungen zunehmend schwierig sei, die Fahrgäste rechtzeitig zu Therapien und Arztbesuchen zu bringen. Diese Anfrage ist nicht aus der Luft gegriffen, denn auch Taxis dürfen diese Spur mitbenutzen.

Der Regierungsrat lehnte das Anliegen trotzdem ab. Weil es sich zusammengefasst in der Güterabwägung nicht rechtfertige, die Busspur für weitere Verkehrsteilnehmer zu öffnen. Als einen Grund nennt Sicherheitsdirektor Beat Villiger gegenüber unserer Zeitung, dass andere Verkehrsteilnehmer verunsichert werden könnten, da Tixi im Gegensatz zu den konzessionierten Taxis über keine Leuchtschilder verfügen würden. Auch heisst es, dass die Verkehrsordnung nicht ausschliesse, «dass mobilitätsbehinderte Personen öffentliche Linienbusse oder kommerzielle Taxis benützen».

Zu lange Fahrzeiten durch Verkehrsprobleme sowie damit verbunden zu hohe Preise für die Fahrgäste, dies waren die Argumente, wieso die Fahrt von Taxis auf der Busspur einst zugelassen wurde. Es ging im weitesten Sinn also um die Existenz der Taxiunternehmen. Das ist immer ein gutes Argument. Die Gesundheit von Menschen mit Behinderungen, die eben nicht auf den Bus ausweichen können und noch weniger als andere keinen Arzttermin verpassen sollten, aber auch. Die Argumente des Regierungsrates überzeugen nicht; dass er sich auf Eigenheiten der Verkehrsordnung stützt, wirkt deplatziert. Zudem kenne ich zumindest niemanden, der nicht fähig ist, ein Tixi Taxi von einem normalen Fahrzeug zu unterscheiden.

Christopher Gilb
christopher.gilb@zugerzeitung.ch

«Es ist ein Katz-und-Maus-Spiel»

Rotkreuz Seit zehn Jahren betreibt das Departement Informatik der Hochschule Luzern die Plattform «eBanking – aber sicher!». Im Auftrag von 100 Banken sensibilisieren Oliver Hirschi und Co. Kunden und Bankmitarbeiter.

Christopher Gilb
christopher.gilb@zugerzeitung.ch

Der neuste Beitrag auf der Plattform «eBanking – aber sicher!» stammt vom 14. September: Eine kritische Schwachstelle im Windows-System ermögliche Angreifern, beliebige Malware – also Schadenssoftware – einzuschleusen, um Daten abzuziehen oder Passwörter auszuspionieren. Abhilfe schaffe das neuste Windows-Update. Nebst solchen Informationen zu Bedrohungen findet man auf der Homepage Tipps, wie man Risiken beim E-Banking maximal vermeidet, und Kursangebote zum Thema. Betrieben wird das Angebot vom Campus Zug-Rotkreuz der Hochschule Luzern. Der 42-jährige Dozent für Informationssicherheit Oliver Hirschi war von Anfang an dabei. Ihm zur Seite stehen zwei wissenschaftliche Mitarbeiter.

Oliver Hirschi, seit zehn Jahren geben Sie Tipps zu sicherem E-Banking. Wie haben sich die Herausforderungen verändert?
Wie immer im Bereich Sicherheit ist auch unsere Arbeit ein Katz-und-Maus-Spiel. Während es vor zehn Jahren noch sicher war, wenn ein Passwort aus acht Stellen, aus Klein- und Grossbuchstaben, einer Zahl und einem Sonderzeichen bestand, genügt das heute nicht mehr. Selbst wir mit unserer eher normalen Technik konnten ein solches in einem Experiment in dreieinhalb Tagen knacken. Deshalb empfehlen wir heute, dass das Passwort mindestens zehn Stellen haben soll. Setzt sich nicht eine gänzlich andere Sicherheitstechnik durch, wird man wohl irgendwann auf elf oder zwölf Stellen erhöhen müssen. Insgesamt ist festzustellen, dass die Kriminellen eben professioneller geworden sind.

Wie äussert sich das?
Nehmen wir Phishingmails, also Mails, um an persönliche Daten zu kommen: Früher wurden diese in schlecht formuliertem Deutsch und willkürlich an Millionen von E-Mail-Adressen verschickt. Heute sind sie häufig in gutem Deutsch formuliert, weil die Kriminellen möglicherweise Verbündete haben oder die Sprache selbst können. Zudem werden sie spezifischer verschickt und sind persönlicher formuliert. Über solche Entwicklungen informieren wir dann fortlaufend Bankkunden und die Banken selbst.

Oliver Hirschi im Besprechungsraum auf dem Campus. Bild: Werner Schelbert (Rotkreuz, 18. September 2018)

Wie läuft Letzteres ab?
Wir werden zwischenzeitlich von rund 100 Banken getragen. Die Aufgabe war von Anfang an, dass diese nicht nur ihre Kunden auf unser Angebot verweisen können, sondern wir auch für die Bank konkret etwas anbieten. Das beginnt mit dem täglichen Medienmonitoring. Wir durchforsten also zeitnah alle grösseren Medien, ob etwas zum Thema Cyberkriminalität im Bereich E-Banking erschienen ist.

Was bringt das?
Früher war oft das Problem, dass Kunden bei ihrer Bank anriefen, weil sie in der Zeitung etwas über neue Cyberattacken irgendwo auf der Welt gelesen hatten, aber die Bank selbst – weil es sich beispielsweise um eine kleinere Regionalbank handelt – den konkreten Fall noch nicht kannte. Heute informieren wir die Banken fortlaufend über aktuelle Probleme und machen Vorschläge, was sie diesbezüglich selbst verbessern könnten, und sensibilisieren Mitarbeiter im Kundenservice entsprechend.

> «Für Cyberkriminelle ist es einfacher, den kleinen Kunden als die grosse Bank anzugreifen.»
>
> **Oliver Hirschi**
> Leiter «eBanking – aber sicher!»

Aber wäre es nicht Aufgabe der Banken, für sicheres E-Banking zu sorgen?
Ein vollkommen sicheres System gibt es nicht, die Bank trägt ihren Teil bei, aber der Kunde ist eben auch Teil des Systems. Er erledigt sein E-Banking beispielsweise über seinen persönlichen Computer. Wie sicher dieser ist, darauf hat die Bank wenig Einfluss. Für Cyberkriminelle ist es viel einfacher, den kleinen Kunden als die grosse Bank anzugreifen. Diese versuchen also entweder, die Hardware des Kunden – etwa mit einem Virus – oder den Kunden selbst zu manipulieren, indem sie sich sein Vertrauen erschleichen – eine Art digitaler Enkeltrick also. Unsere Aufgabe ist die Prävention in diesem Bereich, und befolgt man einige grundlegende Regeln (siehe Box, Anm. d. Red.), ist die Gefahr, dass etwas passiert, auch wirklich klein.

Haben Sie Erfolg?
Unsere zweieinhalbstündigen Kurse sind sehr gut besucht, und was sich sicher feststellen lässt, ist, dass die Leute insgesamt offener für das Thema sind. Das ist sehr erfreulich, denn für die Sicherheit zu sensibilisieren, ist nicht ganz einfach, bei diesem Thema fällt einem eigentlich niemand um den Hals. Vertrauen bildet sicher auch, dass wir eine Hochschule sind. Kämen die Informationen von den Banken selbst, würden viele denken, da werden vielleicht Sachen bewusst beschönigt. Unsere Unabhängigkeit ist uns sehr wichtig, deshalb haben wir beispielsweise auch immer Angebote von Sicherheitssoftwareherstellern abgelehnt, die beispielsweise hofften, dass wir ihr Produkt als Lösung empfehlen.

Welches sind die typischen Fragen, die an den Kursen gestellt werden?
Eine häufige Frage ist, ob man fürs E-Banking einen separaten PC benutzen soll. Das muss man nicht. Eine andere Frage ist die Haftbarkeit bei etwaigen Schäden. Da müssen wir dann aber an die Bank als Vertragspartner der Kunden verweisen.

Informieren Sie auch Firmenkunden?
Wir sind gerade daran, dies noch stärker aufzugleisen. Das Problem ist, dass das E-Banking nur einen kleinen Bereich der Cybersicherheit eines Unternehmens einnimmt. Deshalb ist es wohl vielen zu spezifisch. Wichtig wäre es trotzdem, wir bleiben dran.

Sicheres E-Banking

Tipps Bevor man die E-Banking-Seite seiner Bank aufruft, sollte man sicherstellen, dass man über eine sichere Infrastruktur verfügt, so der Experte Oliver Hirschi vom Departement Informatik der Hochschule Luzern. Es gelte regelmässig ein **Back-up** zu machen, um sich vor Datenverlust abzusichern, eine **aktuelle Virenschutzsoftware** installiert zu haben, um sich vor technischen Bedrohungen, etwa Malware, zu schützen, eine **Firewall** installiert zu haben, die den Netzwerkverkehr von und zum Internet absichert – und sämtliche Programme auf dem aktuellen Stand zu halten. Zudem sei es wichtig, den **gesunden Menschenverstand** anzuwenden. «Bevor der Finger auf die Maus klickt, sollte es im Hirn klicken», erklärt Oliver Hirschi.

Doch auch beim Anwenden der E-Banking-Programme sollte man einiges beachten. So sollte man die **Webadresse** der Bank manuell im Internetbrowser eingeben, also nicht als Link anklicken oder aus den Favoriten abrufen. «Die Favoriten sind nur eine Datei, ein Virus könnte diese abändern, so dass man auf eine ganz andere Seite als beabsichtigt geleitet wird», so Hirschi. Des Weiteren sollte man kurz einen Blick auf die **Adresszeile** werfen, diese sollte grün sein, und man sollte keine Fehlermeldung erhalten. Auch sollte am Anfang «https://» stehen und ein Schlosssymbol abgebildet sein, dies als Zeichen, dass die Verbindung sicher ist. «Und als letzte Regel: Der **DNS-Name** sollte korrekt sein», so Hirschi. Das sei jener Teil der Adresszeile, der beim Verbindungsaufbau schwarz angezeigt wird, dieser sollte auf den Namen der Bank lauten, um sicherzugehen, dass man nicht woanders gelandet ist. Nehme man sich diese Punkte zu Herzen, könne man auch mit gutem Gewissen seine Bankgeschäfte digital tätigen. *(cg)*

Hinweis
Weitere Informationen zum Thema und zu den Kursen: *www.ebas.ch.*

ANZEIGE