

Hacker sind Geschichtenerzähler

Der Kanton Schwyz machte erstmals am Schweizer Digitaltag mit.



Regierungsrat Andreas Barraud hat sich virtuell an die Besucher im «Gaswerk» gerichtet.
Bild: Andreas Seeholzer

Der Kanton Schwyz partizipierte gestern zum ersten Mal am Digitaltag, «um eine Plattform für den Dialog anzubieten, den Austausch zwischen der Öffentlichkeit, der Regierung und der Wirtschaft zu stärken und um zu zeigen, an welchen digitalen Themen in der Region gearbeitet wird». Organisatoren waren das Amt für Wirtschaft und der Verein Schwyz Next.

Die Mittagsveranstaltung des Digitaltags stand im Zeichen von Datenschutz und Datensicherheit. Ivan Bütler referierte im «Gaswerk» darüber, «wie einfach wir gehackt werden». Anhand von Beispielen, unter Einbezug des Publikums und mittels Live-Hacking führte Bütler in die Welt des Datenklaus. Bütler ist Gründer und Geschäftsführer der auf Ethical Hacking und Penetration Testing spezialisierten Compass Security AG mit Sitz in Rapperswil-Jona. Das Unternehmen beschäftigt

heute 55 Mitarbeiter in Bern, Zürich, Rapperswil-Jona, Berlin und Toronto. Bütler wurde vom Bund beigezogen, als Daten vom Eidgenössischen Departement des Innern (EDI) geklaut worden waren und auch im Fall der Ruag.

Wie Bütler ausführte, gibt es zwei Schienen, auf denen ein Datenklau abläuft: eine technische und eine menschliche. Während die technische durch Anwender kaum beeinflusst werden kann, ausser dass Sicherheits-Updates der Hersteller regelmässig heruntergeladen werden, stösst die menschliche Komponente den Hackern Tür und Tor auf.

Die menschliche Komponente und der Fotowettbewerb

Bütler zeigte in seinem Vortrag auf, wie einfach es sein kann, an Natelnummern heranzukommen: «Hier meine Natelnummer, senden Sie mir bitte eine

SMS.» Und schon hatte der Datenklau-Fachmann die Handy-Nummern von 20 der 53 anwesenden Zuhörer auf seinem Mobiltelefon. Und genauso läuft es auch bei einem Angriff von Hackern: «Ein Angreifer ist ein Geschichtenerzähler. Er muss einen Weg finden, damit sein Opfer zu ihm eine Verbindung aufbaut.» Sobald dann das Opfer das vom Hacker versandte Dokument anklickt, öffnet eine im Dokument versteckte Software den Zugang für den Hacker.

Am Beispiel des EDI sagte Bütler, dass den Mitarbeitern das Mitmachen an einem Fotowettbewerb angeboten worden war. Mit einem Anklicken des Fotowettbewerbs waren die Hacker im System des EDA. Was kann also von der menschlichen Seite her gemacht werden, um sich zu schützen? «Klicken Sie keine Dokumente an und verwenden sie möglichst viele Passwörter.» (see)