

# Smartphones im Publikum gekapert

IT-Experte Götz Schartner referierte beim Unternehmerforum der Volksbank Wilhelmshaven



Bewaffnet mit Wissen und Technik: Mit anschaulichen Experimenten verdeutlichte IT-Sicherheitsexperte Götz Schartner (rechts), wie einfach es Cyberkriminellen zuweilen gemacht wird. WZ-FOTO:GIESERS

## **Götz Schartner demonstrierte, wie einfach Datenklau oder das Abhören fremder Smartphones möglich ist. Die Gäste des 10. Unternehmerforums wurden „Opfer“ seiner Attacken.**

Von STEPHAN GIESERS

---

**WILHELMSHAVEN** – Gestohlene Identitäten, gehackte Accounts und fremdgesteuerte Smartphones – die Zuhörer beim 10. Unternehmerforum der Volksbank Wilhelmshaven werden sich am Mittwochabend die analoge Welt mit Wählscheiben zurückgewünscht haben. Götz Schartner, Geschäftsführer der IT-Sicherheitsfirma „8com“, führte den 200 Gästen im Stadttheater live vor, wie schnell sie Opfer von sogenannten Cyber-Kriminellen werden können.

Schon eine SMS öffnete den Gästen die Augen – gefälscht vom Referenten und verschickt an Anwesende: „Liebster Mike, wir müssen vorsichtig sein. Mein Mann ist misstrauisch geworden. Deine Helga.“ Nicht nur Mike und Helga blieb bei Live-Experimenten dieser Art das Lachen im Halse stecken. Gäste schalteten hektisch ihre Smartphones aus. „Zu spät“, sagte Schartner mit schadenfrohem Grinsen. Er habe längst die Signale der Smartphones im Saal abgefangen. Das gehe kinderleicht, da die Geräte automatisch nach W-Lan-Netzen suchten. Die Namen der Smartphones warf der Referent auf eine Leinwand über der Bühne. Mit wenigen Kniffen könne er gar die Kontrolle über die Geräte übernehmen.

In einem weiteren Experiment zeigte Schartner, wie einfach aus dem Smartphone ein Abhörgerät wird. Dafür schickte er zwei Zuhörer mit ihren Handys vor die Tür. Schartner konnte auf die kleine Kamera und das Mikrofon zugreifen, schoss Fotos, belauschte das Gespräch.

Regelmäßige Software-Updates, Passwörter niemals mehrfach verwenden, Kameras in Smartphones und an Computern abkleben – das sind einige Tipps, die er seinen Zuhörern mit auf den Weg gab. „Hacker suchen nach Fehlern“, sagte Schartner und betonte, dass es in fast jedem Netz und in jeder Software Sicherheitslücken gebe.

Den Kriminellen gehe es dabei gar nicht um das Opfer als Person. Das sei auch beim Identitätsdiebstahl nicht der Fall – zum Beispiel bei Ebay. Cyber-Kriminelle bieten über gehackte Ebay-Accounts Waren zum Schnäppchenpreis an und lassen sich das Geld aufs eigene Konto überweisen. Von 500 Bestellern würden im Schnitt 200 bis 300 tatsächlich zahlen, so Schartner. Ware erhielten sie indessen nicht. Leidtragende seien die eigentlichen Account-Inhaber, die plötzlich Mahnungen im Briefkasten oder gar die Polizei vor der Tür hätten.

Oft würden Kriminellen diese und andere Maschen leicht gemacht, da viele Nutzer nur ein einziges Passwort verwenden. Anhand der Website eines Online-Shops verdeutlichte Schartner, wie einfach Nutzerdaten automatisch ausgelesen werden können. Eine spezielle Software sucht dann, ob persönliche Zugangsdaten auch bei anderen Online-Shops und in Datenbanken zu finden sind. Zum Beispiel bei Ebay oder Paypal – „das sind dann absolute Volltreffer“. Wert dieser Handelsware für Kriminelle: Ein Datensatz – 10 Dollar. Nach einer Stunde Arbeit ließen sich so locker 50 000 Dollar verdienen.

Ins Eingemachte ging es, als Schartner mittels Baukastensystem einen Trojaner zusammenbaute und mit einer PDF-Datei verschickte. Leicht modifiziert, könne der Trojaner ein Virenschutzprogramm umgehen. Mit Trojanern würden nicht nur Privatpersonen, sondern auch Netzwerke von Unternehmen gehackt. Allein seine Beratungsfirma habe im vergangenen Jahr drei Fälle mit Schäden im mehrstelligen Millionenbereich betreut – Fälle mit Schäden im sechsstelligen Bereich zähle die Firma im Schnitt zwei pro Woche. Verteufeln wolle er die Digitalisierung gewiss nicht: „Wer die Digitalisierung verschläft, wird irgendwann nicht mehr wettbewerbsfähig sein“, so Schartner. Um so wichtiger, die Sicherheit ernst zu nehmen.

---