USB-Sticks – die Seuche des Jahrhunderts

Frank Puschin, Cybercrime-Spezialist beim LKA, informiert Unternehmerfrauen über Gefahren aus dem Netz

Landkreis Osterholz. Über die vielfältigen Bedrohungen aus dem Internet referierte Frank Puschin, Leiter der Koordinierungs- und Interventionsstelle Cybercrime vom Landeskriminalamt Niedersachsen, vor den Unternehmerfrauen im Handwerk in einem voll besetzten Haus.

„Bringen Sie jeden Cyberangriff auf ihre Firmendaten zur Anzeige“ empfahl der Experte. „Wir kommen nicht gleich mit Blaulicht vorgefahren“, scherzte er, „aber durch ihre vermehrte Anzeige wird an anderer Stelle erkannt, wie nötig eine Befassung der Polizei mit diesen Themen ist. Außerdem ermöglichen Sie uns dadurch, die aktuelle Cyberbedrohungslage besser einzuschätzen und unsere Präventionshinweise zu aktualisieren“, erläuterte Puschin. Er forderte dazu auf, sämtliche Spam-, Phishing- und Trojanermails an die E-Mail-Adresse trojaner@zik-nds.de weiterzuleiten, um die Arbeit der Spezialisten zu unterstützen.

Virenscanner und Firewalls und auf jeden Fall entsprechende Updates bieten zunächst einen grundlegenden Schutz. Um ein Unternehmen regelrecht zu hacken, müssten Cyberkriminelle unter anderem das Betriebssystem und den Softwarestand von einzelnen Programmen kennen. „Dies ist aufwendig, und Cyberkriminelle wählen daher den für sie leichteren Weg und versuchen, per E-Mail-Anhang an die Mitarbeiter ins System einzudringen“, so Puschin.

E-Mails mit schadhaftem Anhang seien daher an der Tagesordnung. Wenn diese dann auch noch von vermeintlich bekannten E-Mail Absendern stammen, sei die Neugierde des Mitarbeiters geweckt und ein unbedachter Klick könne schnell zu einer kompletten Verschlüsselung des gesamten Firmennetzwerkes führen, erläuterte Puschin.

Dies sei zum Beispiel bei der aktuellen Welle von Bewerbungen der Fall, denn dort werde versucht, den Empfänger zum Öffnen des verseuchten Anhangs zu bewegen. Zurzeit sei dieser „sogar“ mit einem Passwort geschützt – wie der Absender vorgebe, aus Datenschutzgründen. „Der wahre Grund ist: Virenscannern soll die Arbeit erschwert werden, da diese verschlüsselte Anhänge nicht scannen und auf Viren prüfen können.“

„Ist auf diesem Wege ein Verschlüsselungstrojaner in das Computersystem eingedrungen, haben Sie keinen Zugriff mehr auf ihre Daten“, fuhr Puschin fort. In der Regel folgten dann Erpressungsschreiben, in denen die Unternehmer aufgefordert würden, einen bestimmten Betrag in der Kryptowährung Bitcoin zu zahlen. Nach erfolgter Zahlung würde eine Entschlüsselungssoftware angeboten, die angeblich den entstanden Schaden beheben könnte.

Puschin verwies in diesem Zusammenhang auf https://zac-niedersachsen.de, die Internetseite der Zentralen Ansprechstelle Cybercrime. Diese Seite sei ein polizeilicher Berater für Firmen, Verbände und Behörden bei der Prävention von Cyberkriminalität und der erste Ansprechpartner im Schadensfall. Hier gäbe es Hilfestellung, Checklisten, Notfallpläne für den Fall eines Cyberangriffes und insbesondere für die Zeit davor, so Puschin. „Sind Sie auf einen Angriff vorbereitet?“ fragte Puschin die Teilnehmer. Wichtig sei, in jedem Unternehmen eine Ansprechperson zu benennen, die für die IT zuständig ist und die Mitarbeiter ständig auf dem Laufenden hält. „Klare Regeln, Standards und Abläufe verbessern das IT-Sicherheitsniveau ihrer Firma“, so Puschin.

„Wie ist die Nutzung von privaten Komponenten, in Ihrem Betrieb geregelt?“ warf Puschin fragend in den Raum. USB-Sticks seien die Seuche des 21. Jahrhunderts. Die Nutzung privater USB-Sticks sollte untersagt werden, meinte der Experte. Eine klare Regelung erfordere auch die Nutzung von privaten mobilen Endgeräten im Firmen-WLAN.

Auch spiele die Zusammensetzung der Passwörter eine Rolle. „Gehören ihre Mitarbeiter zu den 59 Prozent der User, die einen Generalschlüssel für mehrere Konten verwenden?“ Komplexe und vor allem unterschiedliche Passwörter seien der beste Schutz für Onlinekonten und Zugänge, so Puschin. Er empfahl die Nutzung von Passwort-Managern zur Verwaltung der zahlreichen Konten.

Auch über Erfolge konnte Puschin berichten. So sei durch internationale Zusammenarbeit unter anderem ein Callcenter in Indien geschlossen worden, von dem aus Täter mit sogenannten „Microsoft-Support-Anrufen“ Bürgern in Deutschland das Geld aus der Tasche gezogen hätten. Eine Anzeige lohne sich in jedem Fall.