Ausgesperrt ... und jetzt?

SHUTTERSTOCK

Im Prinzip reicht ein fataler Klick, schon sind PC, Smartphone & Co nur mehr gegen Lösegeld in Kryptowährung „freischaltbar". So funktionieren CryptoLocker. Eine fiese Masche, die in Zeiten des „Smart Workings" eine neue Frage aufwirft: Wer haftet eigentlich für den Schaden?

VON JOHANNES VÖTTER

SÜDTIROL War das ein virtueller Angriff als Reaktion auf die Sanktionen, die Italien im Ukraine-Konflikt unterstützt?
Wie auch immer – jedenfalls wird seit dem 23. März, als die Systeme von Trenitalia bzw. Ferrovie dello Stato auch hierzulande teilweise komplett ausfielen, in diese Richtung wild spekuliert. Zumal die Angst vor einer hybriden Konfliktausartung über die Grenzen des Ukrainekriegs hinaus spürbar ist. Doch wie so oft: Meist ist die Ursache trivialer als jede Panikmache. Denn wer an jenem Tag vergeblich auf den Zug wartete, war schlichtweg Opfer einer – erfolgreichen – CryptoLocker-Attacke.

Wenn plötzlich nix mehr geht

Das bestätigte dann auch die Post- und Kommunikationspolizei gegenüber der Nachrichtenagentur ANSA: Die Systeme der Eisenbahnbetreiber waren gehackt worden. Nur gegen Lösegeld in Kryptowährung wäre diese Datensperre aufgehoben worden. Ging es in diesem Fall um einen Geldbetrag im vielstelligen Bereich, so nehmen diese international operierenden, digitalen Erpresserbanden häufig aber auch gerne Kleingeld. Ob Megakonzern, Kleinunternehmer oder Privatperson: Das Prinzip der CryptoLocker-Masche bleibt nämlich dasselbe. Meist reicht das Öffnen eines Anhangs, währenddessen sich eine Schadsoftware *(Anm.: „Malware" oder „Ransomware" genannt)* installiert und in der Folge PC, Smartphone & Co blockiert. Dann bleibt nur mehr eine Lösung: Das Gerät vom Netz nehmen, Festplatten formatieren, das System neu aufsetzen, Back-ups einspielen, sämtliche Passwörter wechseln – und: Unbedingt eine Anzeige erstatten!

Keine falsche Opfer-Scheu!

Dazu rät auch Ivo Plotegher (i.B.), Leiter der Bozner Dienststelle der Post- und Kommunikationspolizei: Nicht erst seit der „Trenitalia-Attacke" würden vermehrt Fälle von Geschädigten gemeldet. Wobei der Südtiroler Online-Ermittler auch beobachtet, dass die „Peinlichkeit der Situation" manche Betroffene mit einer Meldung/Anzeige zögern lasse: „Die User sind sensibilisiert, aber es kann auch in einem Moment der Unachtsamkeit oder des falschen Vertrauens passieren, dass man unbedacht so eine Datei öffnet."
Zumal die digitalen Tätergruppen geschickt mit den Ängsten ihrer potenziellen Opfer spielen. Meist sind es fingierte Nachrichten (per E-Mail, SMS oder Chat) von renommierten öffentlichen Institutionen oder Dienstleistern, die zum Öffnen einer Datei im Anhang oder eines weiterführenden Links verleiten. Und wenn so etwas in einem Unternehmen passiert, kann dies eine Kettenreaktion auslösen – nämlich, dass infizierte Mails intern an Kollegen weitergehen, deren Endgeräte oder Netzwerkzugänge ebenso dieser CryptoLocker-Attacke anheimfallen.

Was ist privat, was beruflich?

Ein Phänomen, das zuletzt wieder bei mehreren Südtiroler Unternehmen zu beobachten war. Und das eine neue Frage aufwirft – vor allem für jene, die einen privaten Schaden oder Datenverlust erlitten haben. Denn auf Tablets und Handys sind die Grenzen zwischen „privat" und „beruflich" fließend.
Darauf angesprochen, antwortet Rechtsanwalt Thomas Schnitzer (i.B.r.): „Der Arbeitgeber haftet für die Sicherheit des Arbeitnehmers – und damit auch für die von ihm für die Arbeit verwendeten Geräte. Darüber hinaus können sich aus Unternehmenssicht auch Fälle der Haftung gegenüber Dritten ergeben. Etwa wenn Kundendaten nicht fachgerecht verwahrt wurden und fahrlässig ein so genannter ‚Data Breach' passiert."

Weil aber diese Trennung – etwa, weil manche Apps nur über Stores erhältlich sind, die wiederum private Daten für den Download benötigen *(Stichwort: Google, WhatsApp & Co)* – gar nicht so einfach ist, sei auf User-Seite Eigenverantwortung gefragt, wie Schnitzer erinnert: „Das beginnt beim steten Aktualisieren der Antivirus-Programme und reicht bis zu den persönlichen Verhaltensweisen im Netz. Fremde Inhalte sollte man nie downloaden, persönliche Informationen nicht an Dritte weitergeben oder in Chats schreiben. Zudem empfiehlt es sich, bei der eigenen Rechtsschutzversicherung auf Deckung solcher Schadensfälle nachzufragen."
Denn: Schadenersatz einzuklagen, ist fast nicht möglich. Und das, obwohl es sich um ein schweres Vergehen handelt: nämlich „digitalen Hausfriedensbruch", der laut Art. 615ter StGB mit ein bis drei Jahren Haft belangt wird. Auch kann Art. 629 StGB („Erpressung") zur Anwendung kommen; dann drohen fünf bis zehn Jahre Haft und eine Geldstrafe von 1000 bis 4000 Euro. Doch wie der Trenitalia-Fall auch zeigt: Die Täter sind de facto kaum auszumachen.

So tappen Sie nicht in die CryptoLocker-Falle

- **Öffnen Sie keine E-Mails voreilig!** Achten Sie immer auf Absender und Inhalt, erst recht, bevor sie Anhänge öffnen oder auf Links klicken.
- **Verwenden Sie den PC und Laptop niemals mit dem Administratorprofil!** So kann man einen ev. Erpressungsversuch später über einen alternativen Benutzer umgehen.
- **Erstellen Sie regelmäßig Sicherungskopien** (Back-ups auf Festplatte und/oder in der Cloud) der wichtigsten Daten und aktualisieren Sie Virenschutz & Co laufend!
- **Verwenden Sie nie USB-Sticks unbekannter Herkunft!**
- Falls Sie Opfer einer CryptoLocker-Attacke wurden: **Zahlen Sie niemals! Erstatten Sie sofort Anzeige!** Bei der Post- und Kommunikationspolizei oder bei jeder Dienststelle von Polizei oder Carabinieri.