Vorsicht, Erpresser im Netz!

Lösegeld Die Erpresser-Software «Petya» richtete unlängst grosse Schäden an. Vor allem Banken, Telekomfirmen und Energieunternehmen waren betroffen. IT-Profi Ivan Bütler erklärte in Ruggell, was die digitalen Erpresser antreibt und was Unternehmen dagegen tun können.

VON DOROTHEA ALBER

Und täglich grüsst das Murmeltier. Hacker erpressen Unternehmen oder Kunden. Kaum hat das eine Schadprogramm grosse Schäden angerichtet, bringen Cyberkriminelle das nächste in Umlauf. «Wanna Cry» zum Beispiel verschlüsselte Dateien und machte so Computer unbrauchbar. Damals verlangten die Hacker 300 Franken von ihren Opfern. Windows-PC auf der ganzen Welt waren betroffen. Die Malware nutzte eine Schwachstelle des Windows-Betriebssystems. Darauf folgte das Schadprogramm «Petya», das die gleiche Schwachstelle des Systems nutzte und Unternehmen erneut um 300 Franken erpresste. «Es ist wie im wilden Westen: Es wird auf alles geschossen, was sich bewegt», erklärt IT-Profi Ivan Bütler. Er referierte unlängst in Ruggell zum Thema «Ransomware». Durch diese Schadprogramme verschlüsseln Hacker Daten auf der Festplatte und fordern dann Lösegeld. Solche Erpressungs-Trojaner gibt es schon länger, doch Experten haben 2016 eine Vervielfachung dieser Malware festgestellt. «Die Haupttäter kommen vor allem aus Brasilien, den Balkan-Staaten und China», erklärt Bütler.

Ivan Bütler testet als «guter Hacker», wie verwundbar Unternehmen sind. Bild: pd

Schwachstelle Mitarbeiter

Auch Schweizer und Liechtensteiner Unternehmen bleiben von Erpressern nicht verschont. Unlängst in die Öffentlichkeit gelangte der Fall der damaligen Valartis-Bank (heute Bendura Bank) in Bendern. Die Hacker drohten mit Datenweitergabe: Sollte nicht gezahlt werden, wollten sie Daten an Finanzbehörden und Medien weiterreichen. Es ist nicht bekannt, wie die Bank damit umgegangen ist. Nur selten gelangen solche Angriffe laut Bütler auch in die Öffentlichkeit. Er erklärte an einer Veranstaltung in Ruggell, wie sich Unternehmen vor solchen Angriffen schützen können. Organisiert wurde der Anlass von proIT als Branchenverband der Sektion Informatik der Wirtschaftskammer Liechtenstein.

Als eine grosse Schwachstelle macht Bütler die Mitarbeiter aus. Denn die Angriffe erfolgen meist nicht von Aussen, sondern zum Beispiel über verseuchte Emails oder USB-Sticks. «Die beste Strategie gegen die steigende Gefahr von Ransomware ist es, eine Back-up-Strategie zu haben», empfiehlt Bütler. Die Sicherung auf einer Netzwerkfestplatte oder einer fest angeschlossenen externen Disk ist riskant. Einige Trojaner können auch diese Medien verschlüsseln. Die Festplatte muss nach jedem Back-up vom PC getrennt werden.

Bitte jetzt aktualisieren!

Vor allem aber sollten Unternehmen ihre Systeme aktuell halten. «Manche werden von Windows automatisch aktualisiert, andere müssen selbstständig von der IT auf dem aktuellsten Stand gebracht werden». Die Firmen müssen es Bütler zufolge in Griff haben, auch alle Zusatzprogramme zu aktualisieren, wie zum Beispiel Adobe oder den Flash Player.

Betroffen sind Unternehmen jeder Branche, allerdings seien KMU am stärksten betroffen, weil sie eine weniger professionelle IT haben. Erpressungs-Trojaner können über den Besuch von Websites auf den Rechner gelangen. Meistens laden sich die Opfer die Malware über E-Mail-Anhänge herunter, die ein gut getarntes Schadprogramm enthalten. Das kann auch eine Word- oder Excel-Datei sein. So zeigte Bütler, wie etwa ein Schadprogramm als Excel-Dokument getarnt ist. Daher ist es Bütler zufolge wichtig, die Mitarbeiter zu sensibilisieren. Richtige Prävention kann grössere Schäden vermeiden.

«Es ist wie im wilden Westen: Es wird auf alles geschossen, was sich bewegt»

Als Sicherheitsexperte hackt sich Ivan Bütler, Gründer der Firma Compass Security, beruflich in die Netzwerke seiner Kunden. Diese «Penetration-Tests» zeigen, wie angreifbar das IT-System eines Betriebes ist. «Einen Trojaner einzuschleusen, funktioniert in 99 Prozent der Fälle. Wenn es per Mail nicht geht, dann verteilen wir gratis USB-Sticks oder verschicken eine CD-ROM per Post», sagt Bütler. Er testet seine Kunden knallhart. So verschickte er im Auftrag eines Schweizer Unternehmens unter dem Betreff «Sex-Party» bereits Test-E-Mails mit dem Hinweis auf anzügliche Fotos der Chefetage. Der Grossteil der Mitarbeiter klickte den Link an.

IT-Spezialisten wie Ivan Bütler sind in der Schweiz begehrt. Er versetzt sich in die Angreifer. Dabei schilderte er in Ruggell, was sich aus seiner Sicht finanziell besonders lohnen würde. Als Hacker würde er börsenkotierte Unternehmen hacken und zum Beispiel Quartalsberichte stehlen, um dann die richtigen Aktientitel kaufen zu können. Das sei eines der grössten Probleme heute. Doch die Motive der Hacker sind unterschiedlich. Während es Cyberkriminelle gibt, die damit Geld erpressen oder versuchen Gelder zu stehlen, hacken viele einfach nur aus Spass. Auf einer Internetseite stellen sie ihre gehackten Webseiten wie Trophäen online. Bütler zeigte, welche Liechtensteiner Seiten in den letzten 24 Stunden erfolgreich gehackt wurden. Doch wenn kriminelle Absichten dahinter stehen, dann entstehen grosse Schäden. Er schätzt, dass sich diese alleine bei seinen Kunden auf 250 000 Franken im Monat und damit auf mehrere Millionen pro Jahr belaufen.

Ivan Bütler selbst ist vorsichtig: Er nutzt zwar Google – allerdings sehr devensif: Er nutzt zusätzliche Sicherheits-Plugins in den Browsern, löscht den Zwischenspeicher regelmässig und unterbindet sogenannte «Trackings» durch Werbung im Netz. Das sei für ihn selbstverständlich, wie er der Schweizer Zeitung TagesWoche verrät. E-Mails verschickt Bütler – «wenn immer möglich» – verschlüsselt. Sein Smartphone sieht er als unsicher an. Er hat daher keine Geschäftsdaten auf dem Handy und keine Verbindungen zu den Rechnern seiner Firma gespeichert.

Er rät zudem, Hardware zu verschlüsseln und sich so vor Diebstahl zu schützen. Unterschiedliche Passwörter seien ratsam. Verdächtige Dateien, die per E-Mail erhalten werden, können Nutzer überprüfen. Dafür empfiehlt er zum Beispiel das Online-Virenprogramm Virus-Total. Mit der Software «Cleondris» könne man zudem prüfen, ob eine Verschlüsselung in Gang ist.

Einige Tipps des Experten

1. Lösegeld zu zahlen, scheint offenbar das Problem für betroffene Unternehmen nicht zu lösen. «Bei Petya gaben Hacker keine Daten zurück, selbst wenn Unternehmen gezahlt haben», erklärt IT-Profi Ivan Bütler.
2. Es gibt ein Ransomeware-Playbook, welches praktisch als Anleitung fungiert, was Unternehmen tun können bzw. wie sie mit Schadprogrammen umgehen sollen.
3. Den infizierten PC oder Server vom Netzwerk, Wifi, LAN trennen.
4. Ursachen beim infizierten PC finden
5. Gibt es andere Geräte mit den gleichen Symptomen?
6. Stoppen der Infektion (Email, Web Proxy, USB-Stick, CD-ROM, Handy)