Was ist Smishing, und wie kann man sich davor schützen?

Haben Sie schon einmal eine SMS auf Ihrem Smartphone erhalten, in der Sie aufgefordert wurden, auf einen Link zu klicken, um weitere Informationen zu erhalten? Es könnte sich um eine Zustellungsmitteilung eines Online-Shops oder eines Postdienstes handeln oder um eine Benachrichtigung über eine neue Voicemail. Vielleicht kam Ihnen die SMS etwas komisch vor, und Sie haben sich gefragt, ob Sie auf den Link klicken sollen oder nicht. Aber Sie wollten wissen, wo Ihr Paket ist oder wer eine Nachricht hinterlassen hat, also haben Sie es trotzdem getan.

Genau das ist der Friseurin und Unternehmerin Loredana Bartels passiert. Sie erhielt eine SMS. Zunächst dachte sie, es sei eine Nachricht von einem neuen Kunden, der einen Termin vereinbaren wollte, doch dann erhielt sie eine weitere SMS, die ihr verdächtig vorkam. Trotzdem klickte sie auf den Link. Nichts schien zu passieren und es gab keine Voicemail. Das beunruhigte Loredana.

Loredana ist nicht die Einzige. Viele andere Kleinunternehmer und Angestellte in der Schweiz sind in letzter Zeit Ziel von SMS-Phishing-Attacken mit dem Namen Flubot geworden. SMS-Phishing – oder anders gesagt Smishing – ist eine Art von Cyberangriff. Dabei werden Sie dazu verleitet, auf einen Link zu klicken oder eine Malware, einen bösartigen Code, zu installieren, der dem Angreifer Zugriff auf Ihr Gerät oder Ihre sensiblen Daten gibt. Er kann zum Beispiel auf Ihre Kontaktliste zugreifen und dann Nachrichten an Ihre Freunde und Geschäftskontakte senden, wobei er vorgibt, Sie zu sein.

Glücklicherweise wusste Loredana, an wen sie sich wenden musste, um sicherzustellen, dass alles in Ordnung war. Die Security Defender des GEIGER-Projekts untersuchten Loredanas Smartphone. GEIGER ist ein von der EU finanziertes Horizon 2020-Innovationsprojekt, das eine Cybersicherheitslösung für kleine Unternehmen entwickelt. Loredana nimmt an dem Projekt teil und hilft den Cybersicherheitsexperten, die Perspektive von Kleinunternehmen zu verstehen. Gemeinsam fanden sie heraus, dass Loredana ihr Smartphone richtig konfiguriert hatte und es der Flubot-Malware nicht gelang, sich zu installieren. Die Einstellungen verhinderten, dass Flubot auf die von Loredana empfangenen Nachrichten zugreifen und Loredanas Kontaktliste zur weiteren Verbreitung nutzen konnte. «Bevor ich überprüft habe, ob sich die Malware auf meinem Telefon installiert hat, hatte ich ein wenig Angst. Was würden sie mit den von mir gestohlenen Telefonnummern machen? Was würde mit meinen Kontakten passieren? Es würde mir sehr leid tun, wenn meine Kunden meinetwegen betroffen wären», sagte Loredana. «Jetzt, wo ich mehr weiss, möchte ich auch meinen Kunden helfen, indem ich sie warne. Ich habe meinen Mitarbeitern bereits geraten, nicht auf solche Links zu klicken.»

Wie können Sie wissen, ob Ihr Smartphone betroffen war? Oder ob Sie selbst gefährdet sind? Wie können Sie verhindern, dass es Cyberkriminellen gelingt, durch einen Smishing-Angriff auf Ihr Smartphone zuzugreifen? Es gibt ein paar einfache Maßnahmen, die Sie ergreifen können. Prüfen Sie zuallererst, dass keine unbekannten Apps installiert werden dürfen. iPhones sind immer so konfiguriert. Android-Telefone bieten diese Einstellung im Menü «Biometrie und Sicherheit».

Wenn Sie eine Flubot-SMS erhalten und auf den Link geklickt haben und Ihr Telefon die falschen Einstellungen hat, die die Installation unbekannter Apps zulassen:

1) Aktivieren Sie den Flugmodus Ihres Smartphones.
2) Überprüfen Sie alle Online-Dienste, die eine SMS-Anmeldung verwenden (Zwei-Faktor-Authentifizierung), dass nichts Böses passiert ist.
3) Melden Sie den Vorfall Ihrem lokalen Cybersicherheitszentrum (in der Schweiz ist dies die NCSC)
4) Sichern Sie Ihre wichtigen Daten.
5) Setzen Sie Ihr Telefon zurück.
6) Überprüfen Sie die Einstellungen, die verhindern, dass unbekannte Apps installiert werden.

«Es wäre wichtig, gewarnt zu werden, wenn ein Angriff wie Flubot im Umlauf ist, um vorbereitet zu sein. Und da ich kein Cybersecurity-Experte bin und nicht weiß, wie man mit neuen Bedrohungen umgeht, wäre es auch beruhigend zu wissen, dass es qualifizierte Unterstützung gibt, wenn etwas passiert», sagte Loredana.

Möchten Sie, wie Loredana, mehr über digitale Sicherheit erfahren und wie Sie Ihr Unternehmen schützen können? Dann sollten Sie sich bei GEIGER **https://project.cyber-geiger.eu/news.html** anmelden!

Das Projekt «GEIGER» wird unter der Führung der Fachhochschule Nordwestschweiz FHNW mit Partnern aus der Schweiz, Deutschland, Frankreich, Italien, der Niederlande, Spanien, England, Rumänien und Israel durchgeführt. In der Schweiz werden Pilotprojekte mit der Berufsfachschule BBB in Baden und dem Schweizerischen KMU Verband SKV durchgeführt. Finanziert wird das Projekt über das Europäische Forschungsprogramm «Horizon 2020».

GEIGER

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883588 (GEIGER). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.