Phishing- und Awareness-Kampagne

Globales Security-Training für Victorinox

Die Mitarbeitenden von Victorinox rund um den Globus sind heute versiert im Umgang mit potenziell gefährlichen E-Mails. Unter anderem helfen Trainings von Lucy Security und terreActive bei der Sensibilisierung.

→ **VON MARK SCHRÖDER**

Victorinox steht seit mehr als einem Jahrhundert für Schweizer Ingenieurskunst und Präzision. Die weltbekannte Herstellerin des Schweizer Taschenmessers aus dem Kanton Schwyz hat hohe Ansprüche an Design und Produktion. Mindestens ebenso viel Wert legt das Unternehmen auf die Cyber Security. Einerseits wegen eines möglichen Imageschadens bei einem Cyberangriff, andererseits aber auch, weil Konstruktionspläne in die Hände von Kriminellen fallen könnten. Denn im hektischen Arbeitsalltag kann es leicht vorkommen, dass ein Mitarbeitender versehentlich in einer E-Mail auf einen gefährlichen Link klickt und auf einer fingierten Website landet, die versucht vertrauliche Daten abzugreifen.

Keines dieser Szenarien wollten die Verantwortlichen bei Victorinox erleben. «Aufgrund wiederholter Medienberichte über die Gefahr von Phishing und deren möglichen Folgen mit Ransomware-Attacken, konnte die Geschäftsleitung motiviert werden, mehr in die Benutzersensibilisierung zu investieren», sagt Tobias Hauser, Head of Information Security bei Victorinox. Er hatte die User zuvor sporadisch auf die möglichen Gefahren aufmerksam gemacht. Echte Phishing-Tests habe es allerdings nicht gegeben, so Hauser.

DIE MENSCHLICHE FIREWALL

Victorinox beschäftigt am Hauptsitz in Ibach SZ und in zwölf Ländervertretungen weltweit über 2000 Mitarbeitende. Jeder einzelne von ihnen kann einen wertvollen Beitrag zum Cyberschutz leisten, wenn sie oder er die Gefahr frühzeitig erkennt und entsprechend handelt. «Angesichts der rasant steigenden Zahl von Cyberangriffen sollte jeder Betrieb diese menschliche Verteidigungslinie als festen Bestandteil seiner IT-Strategie mit einplanen», ist Hauser überzeugt. Zudem seien Security-Awareness-Projekte immer auch ein Zeichen der Wertschätzung gegenüber den Mitarbeitenden, die sich gut geschult sicherer fühlen können – bei der Arbeit und im Privatleben.

Noch bevor ein Hackeralarm ausgelöst wurde, entschied sich Victorinox zu handeln und das Sicherheitsdispositiv zu erhöhen. Im Frühjahr 2020 begann das Security-Team von Hauser mit der Evaluation von drei Anbietern. «Um rasch mit Benutzerschulung und Phishing-Kampagnen loslegen zu können, haben wir eine Cloud-Lösung gesucht», erinnert sich der Head of Information Security. Ein Hauptkriterium sei gewesen, die Kampagnen und Trainings in acht verschiedenen Sprachen durchführen zu können. Denn, so die Überlegung: Wenn die Benutzer eine Schulung in ihrer Muttersprache absolvieren können, haben sie den grössten Nutzen davon.

Im Sommer 2020 fiel der Entscheid zugunsten des Schweizer Anbieters Lucy Security. Als Partnerin kam terreActive hinzu, die mit der Cloud-Lösung bereits mehrere erfolgreiche Projekte realisiert hatte. Victorinox beauftragte die Aarauer Firma mit dem Aufsetzen von Lucy und der Unterstützung während des mehrstufigen, rund einjährigen Projekts. «Victorinox konnte vom grossen Erfahrungsschatz der terreActive profitieren und zielgerichtete Phishing-Kampagnen rasch ausrollen. Bei der Auswertung der Ergebnisse wurde Unterstützung geboten, sodass das weitere Vorgehen laufend bestimmt werden konnte», kommentiert Hauser die Zusammenarbeit.

PHISHING-SIMULATION AUS DER BOX

Das Cyber-Defence-Konzept von Victorinox baute auf zwei Teilbereichen auf: Erstens die «Phishing-Simulation», für die terreActive mehrere Vorlagen von der Lucy-Security-Plattform auswählte. Es folgten ein Review durch Victorinox und ein Test mit bestimmten Szenarios. Anschliessend startete terreActive die erste Simulation in einem globalen Roll-out: Dabei wurden fingierte E-Mails in acht

Bild: Victorinox

Im neuen Distributionszentrum von Victorinox in Seewen sind 40 Angestellte beschäftigt

Sprachen rund um die Welt verschickt. Dieses Szenario zielte darauf ab herauszufinden, wie gut die Benutzer bereits Gefahren wie gefährliche E-Mail-Anhänge oder gefälschte URLs erkennen konnten. Im Laufe des Projektes wurde der Versand mit neuen E-Mail-Vorlagen und erhöhtem Schwierigkeitsgrad wiederholt, sodass Mitarbeitende mehrmals auf die Probe gestellt wurden und die Erfolgsentwicklung beobachtet werden konnte.

Die Spezialisten von terreActive empfahlen grundsätzlich, Social-Engineering-Kampagnen als wiederkehrenden Prozess zu etablieren, um das Security-Bewusstsein und die -Maturität kontinuierlich zu erhöhen.

E-LEARNING FÜR MEHR SICHERHEIT

Der zweite Teil des Konzepts umfasste «Awareness-Schulungen», die ebenfalls global ausgerollt wurden. terreActive schlug Victorinox hierfür einige Trainingseinheiten vor, die Lucy Security als E-Learning für Firmen anbietet. Auf der Plattform kann der Kunde interaktive Online- und Offline-Schulungen in 30 Sprachen auswählen, darunter Aufklärungsmails, Lernfilme, Websitevorlagen usw. Durch die Schulungen wurden die Mitarbeitenden aktiv mit einbezogen und mit Gefahren vertraut gemacht. Zudem erfuhren sie, wie sie auf Phishing-Attacken reagieren sollen.

Die kleinen Testeinheiten am Ende der Lektionen zeigten sowohl den Mitarbeitenden als auch dem Head of Information Security, wie sich das Sicherheitsbewusstsein entwickelte. Hausers Resümee: Während des rund einjährigen Projektes konnte die IT-Sicherheitskultur bei Victorinox kontinuierlich optimiert werden.

PHISHING IN DER LANDESSPRACHE

Wie der Security-Verantwortliche zugibt, waren während des Projekts und auch im Nachgang noch einige Hürden zu nehmen. «Den zeitlichen Aufwand für die Übersetzung in acht Sprachen und das Testing der Kampagnen haben wir zunächst unterschätzt», sagt er. Auch die Auswertung der Kampagnen nach Abteilungen und Ländern seien anspruchsvoll und zeitintensiv gewesen, wobei terreActive sein Team mit zusätzlicher Manpower unterstützt habe.

Aber auch der Cyber-Security-Dienstleister gibt zu, dass für ihn die Internationalität des Projekts eine besondere Herausforderung gewesen sei. Global tätige Unternehmen entschieden sich oftmals dafür, Sicherheitsprojekte nur in Englisch und mit nur einem Szenario für alle Länder auszurollen. Wie terreActive-CEO Urs Rufer weiss, «ist die Aufmerksamkeit der Mitarbeitenden bei Trainingskampagnen in fremden Sprachen oft geringer». Victorinox entschied sich hingegen, auf die lokalen Gegebenheiten Rücksicht zu nehmen. So werde die Cyber Security gestärkt, ein langfristiger Schutz aufgebaut und auch die Mitarbeitenden motiviert, lobt Rufer.

Victorinox ist nach den Kampagnen und Trainings aber noch nicht am Ziel. Anfang Jahr ist noch eine automatisierte Lösung für die Phishing-Kampagnen etabliert worden. Hausers Ziel war, die internen Personalressourcen nicht zu stark zu strapazieren. Um die Arbeitslast auch der Angestellten nicht übermässig zu erhöhen, empfiehlt er, eher auf Micro-Trainings mit einer Dauer von einer Minute oder kürzer zu setzen. Denn solche Szenarien seien auch im Alltag eher realistisch. ←