Prävention für Cyber-Angriffe mit Audit und Awareness-Schulung

terreActive prüfte und sensibilisierte die Regionalbank SLM auf digitale Schwachstellen

Attacken auf Website und Online-Anwendungen, Verlust von vertraulichen Kundendaten – für jede Firma ein bedrohendes Szenario. Deshalb liess die Bank SLM ihre Webapplikationen durch ein Audit prüfen. Zudem bat sie die terreActive die Mitarbeitenden der Bank auf verschiedene Gefahrenszenarien mit simulierten Angriffen in Form von Phishing vorzubereiten.

Rückblick Mai 2017:
Der Regionalbank SLM aus Münsingen (zwischen Bern und Thun) stehen zwei wichtige Meilensteine bevor: Eine optimierte Website wird zusammen mit einem neuen Partner lanciert. Gleichzeitig kommt eine neue Online-Applikation für die Verwaltung von Kundenanlässen zum Einsatz. Zwei Änderungen, die akute Gefahren für Cyber-Attacken bergen.

Prävention statt Reaktion

Die Bank SLM holte sich Unterstützung bei der terreActive. Neben den Kenntnissen über Security-Audits, brachte terreActive auch ihre Erfahrung aus dem Bankenumfeld mit ein.

«Die gezielte Phishing-Attacke im Rahmen der Security-Awareness-Kampagne war für uns alle eine lehrreiche Erfahrung. Dank diesem Beispiel von Social Engineering wissen wir, wie ein Angriff aussehen könnte – und dass wir darauf vorbereitet sind.»

Fabio Semadeni, Leiter Services

BANKSLM

Für das Projekt wurden folgende Ziele definiert:

- Schwachstellen in der IT-Infrastruktur finden, mit Fokus auf Website und Online-Applikation.
- Die Mitarbeitenden hinsichtlich Cyber-Bedrohungen sensibilisieren, mit Schwerpunkt auf Datendiebstahl durch Phishing-Mails.

Mehrstufiges Vorgehen

Angriffspunkt Technik: Penetrationstest
Im ersten Teil des Auftrages, der Prüfung der Website und der neuen Online-Applikation, führte terreActive ein Audit nach OWASP Top10 Standard mittels manuellen Penetrationstest durch. Durch die gezielte Attacke auf die Webapplikation, wurden Schwachstellen rechtzeitig aufgedeckt und Massnahmenempfehlungen konnten umgesetzt werden, bevor der Hacker angreifen konnte.

Angriffspunkt Mensch: Phishing
Die Mitarbeitenden der Bank SLM sind schon grundsätzlich sehr gut im Umgang mit sensiblen Kundendaten geschult. Aber die immer raffinierteren Methoden der Hacker machen regelmässige Überprüfungen zur Pflicht. Auch in Bezug auf organisatorische Aspekte wie Abläufe und Schnittstellen im Unternehmen lohnt sich eine periodisch durchgeführte kritische Betrachtung. In diesem Projekt führte terreActive die Überprüfung der Awareness mittels Phishing durch.

Phishing ist eine Form von Social Engineering, bei der versucht wird, durch gefälschte E-Mails an vertrauliche Daten zu gelangen. Der Phishing-Angriff bei der Bank SLM erfolgte auf besonders gefährdete Mail-Empfängergruppen. Eine darauffolgende Infizierung mit Malware wäre ein weiteres Szenario.

Die Mitarbeitenden erlebten so unmittelbar, mit welchen Methoden Angreifer an Informationen kommen. Eine Awareness-Schulung, die terreActive im Anschluss an das Projekt für die Mitarbeitenden der Bank organisierte, thematisierte die identifizierten Schwachstellen und Stolperfallen.

Phishing bleibt gefährlich: Kosten und Imageschaden

Mails mit unbekanntem Absender, verdächtig wirkendem Betreff oder ungewöhnlichem Anhang: Phishing ist bekannt – trotzdem gibt es immer wieder betroffene Unternehmen und der Schaden, den es anrichtet, ist beträchtlich. Kontrollierte Angriffe und präventive Awareness-Schulungen bei Mitarbeitenden verhindern einen Ernstfall mit Umsatzausfall, Infrastrukturkosten und Imageschaden.

Warum sich ein Audit lohnt

- Die Sicherheitsinfrastruktur wird von unabhängiger Stelle überprüft.
- Schwachstellen gegenüber Hackerangriffen werden aufgezeigt und beseitigt.
- Ein Massnahmenplan hilft bei der Umsetzung.
- Die Webpräsenz wird abgesichert.
- Das Unternehmen wird gegenüber potentiellen Bedrohungen durch Phishing sensibilisiert.
- Die Security Awareness steigt durch geschultes Personal.
- Sensiblen Daten werden besser geschützt.

Tools im Einsatz: LUCY Software made in Switzerland

Für dieses Projekt setzte terreActive die Phishing Software von LUCY ein, die durch Simulation von realistischen Angriffen die IT-Sicherheit auf den Prüfstand stellt. LUCY erledigt die Erstellung und den Versand der E-Mails, stellt Landingpages und Trainingswebsites zur Verfügung sowie das ganze Berichtswesen. Das Audit-Team der terreActive ist Partner des Schweizer Unternehmens LUCY Security.

BANKSLM

einfach persönlich

Die Bank SLM ist mit mehr als 30'000 Kundinnen und Kunden, rund 70 Mitarbeitenden und 5 Geschäftsstellen stark in die Region zwischen Bern und Thun verankert. Sie wurde 1870 gegründet und betreut sowohl Privat- wie auch Firmenkunden.

www.bankslm.ch

Untersuchungsumfang und -inhalt

Zu Beginn eines Audits wird festgelegt, welcher Bereich in welchem Umfang wie untersucht werden soll. Mögliches Beispiel:

Organisation			Technik		
Bereich	Review	Test	Extern	Intern	Ebene
Konzepte			√√	√	Applikation
Policies				√	System
Prozesse	√			√	Netzwerk
Awareness	√	√			Physische