VERBAND

ANTI-PHISHING MASSNAHMEN: BRANCHENEMPFEHLUNG FÜR E-MAIL-ANBIETERINNEN

Worum es geht

Phishing-E-Mails sind ein grosses Einfallstor für die zunehmenden Cyber-Attacken, denen Unternehmen und Privatpersonen in der Schweiz ausgesetzt sind. E-Mail-Dienste-Anbieterinnen sind die erste Anlaufstelle für deren Kundinnen und Kunden* im Zusammenhang mit Phishing-E-Mails. Phishing-Attacken verursachen daher einen wachsenden Aufwand bei den Dienste-Anbieterinnen. Ausserdem können sie bei deren Kundinnen und Kunden enorme Schäden anrichten. Dennoch ist es in der Praxis kaum möglich, Angreifer zu identifizieren und sie rechtlich zu belangen.[1]

Die vorliegende Branchenempfehlung von Swico zeigt die konkreten und standardisierten Massnahmen der Schweizer Anbieterinnen von E-Mail-Diensten gegen Phishing-E-Mails auf. Sie wird unterstützt vom Schweizerischen Verband der Telekommunikation (Association Suisse des Télécommunications asut), dem Nationalen Zentrum für Cybersicherheit (National Cyber Security Centre NCSC), der Swiss Internet Security Alliance (SISA) und der SWITCH. Damit sollen die Anbieterinnen ihre Kunden besser vor Phishing-E-Mails schützen und die zuständigen Behörden bei der Identifizierung und Verfolgung von Angreifern unterstützen.

Mit den empfohlenen Massnahmen folgt Swico den geltenden Regelungen des Schweizer Rechts zur Filterung und Unterdrückung von unerlaubten Spam-E-Mails und zur Herausgabe von Informationen an Behörden und Gerichte. Ausserdem nutzen die Massnahmen rechtliche Spielräume für konkrete Verhaltensempfehlungen zur Erkennung und Prävention von Phishing-Versuchen sowie zur Information von Kunden über die ergriffenen oder möglichen Massnahmen. Die Branchenempfehlung soll Anbieterinnen als Orientierungshilfe dienen zur Beurteilung der möglichen und angemessenen Massnahmen gegen Cyber-Attacken über Phishing E-Mails.

A. Bedarf und Zielsetzung

1 Phänomen Phishing

«Phishing», zusammengezogen vom englischen «password», «to harvest» und «to fish», bezeichnet den Versuch, über gefälschte E-Mails, Textnachrichten oder Webseiten sensitive Daten, wie Passwörter oder Kreditkartendaten, zu erhalten. Diese Branchenempfehlung beschränkt sich auf das weitverbreitete Angriffswerkzeug der E-Mails. In einer Phishing-E-Mail unterbreitet der Absender meist ein verlockendes Angebot oder setzt den Empfänger unter Druck, ein gefälschtes Formular auszufüllen, den Link zu einer gefälschten Webseite anzuklicken oder einen infizierten Anhang zu öffnen (sogenanntes «Social Engineering»).

2 Rechtlicher Schutz gegen Spam E-Mails nicht ausreichend

Das geltende Recht verbietet Spam E-Mails und damit zumindest indirekt auch massenhaft versandte Phishing-E-Mails. Spam E-Mails gelten als «unlautere Massenwerbung» (Art. 3 lit. o Bundesgesetz gegen den unlauteren Wettbewerb, UWG, i.V.m. Art. 45a Fernmeldegesetz, FMG). Anbieterinnen sind verpflichtet, Kundinnen und Kunden durch Massnahmen nach dem Stand der Technik vor dem Erhalt von Spam E-Mails zu schützen (Art. 83 Abs. 1 Verordnung über Fernmeldedienste, FDV, SR 784.101.1), d.h. Spam-Filter einzusetzen. Auch dürfen die entsprechenden Nachrichten unterdrückt werden (Art. 83 Abs. 2 FDV).

[1] Siehe dazu: iBarry, Phishing: Das E-Mail mit dem Köder, besucht am 11. März 2021, verfügbar unter https://www.ibarry.ch/de/risiken-im-internet/phishing/.

Phishing-E-Mails sind jedoch nicht in jedem Falle Massen-E-Mails. Immer häufiger erfolgen Angriffe durch Versuche, Angehörige einer bestimmten Organisation durch gezielte Ansprache und dem Vortäuschen der Identität einer dem Empfänger bekannten Person (z.B. Vorgesetzte) in die Irre zu führen. Zwar erfüllen Angreifer Straftatbestände (vor allem Betrug, betrügerischer Missbrauch einer Datenverarbeitungsanlage, unbefugte Datenbeschaffung), doch sind die Mittel der Strafverfolgung gegen die anonym, meist aus dem Ausland, agierende Täterschaft wirkungslos. Das geltende Recht bietet den Anbieterinnen aber den notwendigen Spielraum, Massnahmen gegen Phishing-Attacken zu ergreifen und damit Risiken für ihre Kunden zu reduzieren.

3 Ziele der Massnahmen

Kundinnen und Kunden sollen möglichst wenig in Kontakt kommen mit Phishing-E-Mails, um Schäden bei ihnen und hohen Support-Aufwand bei der Anbieterin zu vermeiden. Dazu dienen der Einsatz von Filtern sowie das Unterdrücken oder Entfernen von Phishing-Nachrichten.

Der Informationsaustausch zwischen Anbieterinnen und involvierten Behörden (insbesondere den Strafverfolgungsbehörden und dem NCSC) soll verbessert werden. Damit wollen die Anbieterinnen die Behörden bei der Identifizierung und Verfolgung von Cyber Angreifern unterstützen und zur Verbesserung der Datengrundlage für Filter beitragen.

Die Anbieterinnen sollen ihre Kundinnen und Kunden sensibilisieren, damit diese Phishing-E-Mails erkennen und Schäden bei sich selber oder Dritten, einerseits, sowie hohen Support-Aufwand bei den Anbieterinnen, andererseits, zu vermeiden helfen.

Kundinnen und Kunden sollen transparent über die Schutzmassnahmen der Anbieter gegen Phishing-E-Mails informiert werden. Auch dazu dienen die Sensibilisierungs- und Informationsmassnahmen und die Verträge bzw. AGB mit den Kunden.

B. Massnahmen

1 Direkter Schutz der Kunden vor Phishing-E-Mails

a) Einsatz von Filtern für die Identifikation von Phishing-E-Mails

Rechtlicher Rahmen:
Das Durchsuchen von E-Mails mittels dem Stand der Technik entsprechenden Filtern zur Verhinderung von Spam ist in der Schweiz explizit erlaubt bzw. für Fernmeldedienstanbieter sogar eine Pflicht. Spam-Filter sollen erweitert werden, um die massenweise versandten Phishing-E-Mails zu identifizieren.

Für das Durchsuchen von E-Mails gilt das Fernmeldegeheimnis des Absenders und des Empfängers, sofern der Empfänger oder die Empfängerin das Postfach noch nicht geöffnet hat. Als nicht verschlossene Sendung sind E-Mails von der Anbieterin durchsuchbar, sofern die Abwehr von Gefahren für den Kunden und Dritte diese Massnahme rechtfertigt. Für Phishing E-Mails, die unter Spam fallen, können daher auf der bestehenden rechtlichen Grundlage Filter erweitert und angewendet werden.

Personendaten der Betroffenen (d.h. der Empfänger und der potentiellen Opfer) unterstehen dem Datenschutz. Kundinnen und Kunden sind über den Einsatz dieser Filter in den Verträgen zu informieren. Die Phishing-Filter sollen dabei möglichst wenig Personendaten verwenden. Die für die Filter notwendigen Muster sind auf Basis anonymisierter oder mindestens pseudonymisierter Daten zu erstellen. Für die Filterung notwendig ist die Verwendung von IP-Adressen der Server, von denen Phishing Mails versandt werden. Damit lässt sich eine DNS-basierte Block-Liste («DNSRBL») erstellen. DNSRBL können andere relevante Merkmale verwenden, z.B. bekannte Phishing-Domains oder die E-Mail-Adressen von kompromittierten Absendern. Zulässig ist auch die Verwendung von E-Mail-Header-Merkmalen, soweit diese nicht direkt auf eine Person schliessen lassen.

Vertragliche Regelungen zwischen Anbieterin und Kunden schaffen Transparenz, vermeiden Missverständnisse seitens der Kundinnen und Kunden und erhöhen die Rechtssicherheit. Die Aufnahme einer entsprechenden Vertrags- bzw. AGB-Bestimmung ist daher empfohlen.

Der allfällige Beizug von Dritten als Dienstleister ist schriftlich zu regeln. Dabei ist sicherzustellen, dass Dritte sich bei der allfälligen Bearbeitung von Personendaten an diejenigen Grenzen halten, die auch für die Anbieterin gelten.

Technische Umsetzung:

- Der Einsatz von DNSRBLs bzw. Real-Time-Block-Lists («RBL») ist empfohlen. Auswahl und Einsatz sind vorgängig und regelmässig zu überprüfen.
- E-Mails von nichtexistierenden (NX) Domain-Namen sollten abgelehnt werden, auch wenn der NX Domain-Name im «from»-Feld benutzt wird.
- E-Mails, die URL gemäss SISA-Feed bekannter Phishing-Webseiten enthalten, sollten abgelehnt werden.

b) Unterdrücken von Phishing-E-Mails

Rechtlicher Rahmen:
Noch nicht zugestellte E-Mails unterstehen dem Fernmeldegeheimnis. Anbieterinnen dürfen massenweise versendete Phishing-E-Mails unterdrücken, damit die Kunden diese nicht erhalten. Die Anbieterin ist sogar verpflichtet, Kundinnen und Kunden technische Massnahmen anzubieten, um diese vor Spam zu schützen. E-Mails, die «unlautere Massenwerbung» (Spam) darstellen, dürfen vom Fernmeldedienstanbieter unterdrückt werden, d.h. sie sollen nicht in das Postfach von Kundinnen und Kunden ausgeliefert werden.

Es ist den Anbieterinnen empfohlen, Kundinnen und Kunden über die Möglichkeit der Unterdrückung von Phishing-E-Mails zu informieren und die Verträge bzw. AGB durch eine entsprechende Bestimmung zu ergänzen.

Technische Umsetzung:
Die als Phishing-E-Mails identifizierten Nachrichten werden, falls möglich, direkt vom äussersten, empfangenden Mailserver während der Verbindung zurückgewiesen. Aktuelle RFC-Vorgaben sind dabei zu beachten.

Alternativ werden sie in einen separaten, entsprechend gekennzeichneten Ordner (z.B. SPAM oder analog) des Kunden-E-Mail-Kontos verschoben, statt in den Posteingang der Kundinnen oder Kunden ausgeliefert zu werden.

c) Entfernen von Phishing-E-Mails

Rechtlicher Rahmen:
Sind Phishing E-Mails bereits in das Postfach des Kunden ausgeliefert, von diesem aber noch nicht geöffnet worden, greift das Fernmeldegeheimnis für das Entfernen/Verschieben dieser E-Mails. Dabei wäre eine Bekanntgabe an Dritte problematisch, sofern z.B. im Rahmen eines Strafverfahrens die Voraussetzungen für eine Überwachung nicht gegeben sind. Das Fernmeldegeheimnis steht der Anwendung von Phishing-Filtern nicht entgegen, um Kundinnen und Kunden vor Phishing-E-Mails zu schützen. Sobald diese durch Öffnen des Postfachs selbst entscheiden können, was sie mit den zugestellten E-Mails machen, greift das Fernmeldegeheimnis nicht mehr.

Vertragliche Regelungen über die Zustellung und den Verbleib von E-Mails im Posteingang und auf dem Server bzw. über das Analysieren und Verschieben von Nachrichten aus dem Posteingang sind empfohlen, um das Restrisiko einer Verletzung des Fernmeldegeheimnisses gegenüber von Kundinnen und Kunden zu minimieren und möglichen Überraschungen der Kunden mit entsprechendem Vertrauensverlust gegenüber der Anbieterin zu begegnen.

Personendaten auf dem Server der Anbieterin unterstehen dem Datenschutz. Da in der Regel auch Personendaten von der Filterung und Entfernung betroffen sind, sind Kundinnen und Kunden über solche Massnahmen auch aus datenschutzrechtlicher Sicht transparent zu informieren (mindestens in den AGB, einer Datenschutzerklärung oder als anderweitiger Teil der jeweiligen Vertragsdokumentation).

Der allfällige Beizug von Dritten als Dienstleister ist schriftlich zu regeln. Dabei ist sicherzustellen, dass Dritte sich bei der allfälligen Bearbeitung von Personendaten an diejenigen Grenzen halten, die auch für die Anbieterin gelten.

Technische Umsetzung:
Die als Phishing-E-Mails identifizierten Nachrichten können standardmässig aus dem Posteingang der Kundinnen und Kunden in einen separaten, entsprechend gekennzeichneten Ordner (z.B. SPAM oder analog) verschoben werden.

d) Verwendung von Standards zur E-Mail-Sicherheit

Technische Umsetzung:
Vorhandene Standards zur Reduzierung von E-Mail-Missbrauch (z.B. Sender Policy Framework «SPF», Domain-based Message Authentication, Reporting and Conformance «DMARC» und DomainKeys Identified Mail «DKIM») sollten beim Senden und Empfangen von E-Mails eingesetzt werden. Insbesondere sollten SPF, DKIM und DMARC für einkommende E-Mails genutzt und basierend auf der vom Domain-Halter veröffentlichten Policy gefiltert werden.

Es ist den Anbieterinnen empfohlen, die Best Practices der Messaging Malware Mobile Anti-Abuse Working Group («M3AAWG») zu berücksichtigen. Diese beinhalten Massnahmen für das Versenden, Filtern beim Empfang und zum Schutz der E-Mail-Infrastruktur (https://www.m3aawg.org/published-documents).

e) Information der Kunden und vertragliche Regelungen

Kundinnen und Kunden sind über die Massnahmen Filterung, Unterdrücken und Entfernen von Phishing-E-Mails zu informieren. Es ist empfohlen, auch in den Verträgen bzw. AGB entsprechende Regelungen vorzusehen (vgl. den Mustertext in Ziff. 4 unten).

2 Koordination mit anderen Anbietern und Behörden

a) Meldung von Phishing-Versuchen

Rechtlicher Rahmen:
Zur Unterstützung der Verfolgung von Phishing-Kampagnen können Anbieter sich mit den zuständigen Behörden über festgestellte Phishing-Versuche austauschen.

Die Personendaten der Empfänger von Phishing-E-Mails sind vor der Weiterleitung soweit möglich zu anonymisieren, sofern die Verfolgung von Phishing-Kampagnen damit nicht vereitelt wird.

Kundinnen und Kunden sind über die Möglichkeit der Weitergabe von E-Mails durch die Anbieter transparent zu informieren. Die Anbieter machen diese zudem darauf aufmerksam, dass Kundinnen und Kunden selbst Phishing-URL melden können über antiphishing.ch bzw. einer von der Anbieterin zur Verfügung gestellten Meldeadresse.

Technische Umsetzung:
Anbieterinnen leiten dem NCSC identifizierte Phishing-E-Mails über reports@antiphishing.ch weiter und/oder melden festgestellte Phishing-URL über antiphishing.ch (oder eine entsprechende API).

b) Implementierung und Beteiligung an Filter-Datenbanken

Rechtlicher Rahmen:
Zur Verbesserung der Filtermöglichkeiten können Anbieter sich (auch automatisiert) untereinander und mit den zuständigen Behörden über festgestellte Phishing-Versuche austauschen.

Die Personendaten der Empfänger von Phishing-E-Mails sind soweit möglich zu anonymisieren.

Kundinnen und Kunden sind über die Filter und deren Verbesserung durch den Austausch transparent zu informieren.

Technische Umsetzung:
Den Anbieterinnen ist empfohlen, die von SISA betriebenen Sperrliste unter https://fuchur.switch.ch zu verwenden und sich daran zu beteiligten (ggf. mit Meldung über die entsprechende API).

3 Sensibilisierung der Kunden

Anbieterinnen sollen Kundinnen und Kunden über geeignete Kanäle (z.B. eigene Webseite, Mitteilung im Control Panel) auf das Risiko von Phishing-E-Mails aufmerksam machen und ihnen Massnahmen zur Abwehr von Cyber-Attacken über Phishing-E-Mails empfehlen. Um eine möglichst einheitliche und umfassende Information der Kundinnen und Kunden zu gewährleisten ist empfohlen, insbesondere auf folgende Ressourcen hinzuweisen und diese in geeigneter Weise zu verlinken:

- ibarry.ch der SISA, unter https://www.ibarry.ch/de/risiken-im-internet/phishing;
- Schweizerische Kriminalprävention SKP, unter https://www.skppsc.ch/de/themen/internet/phishing/ und https://www.skppsc.ch/de/wp-content/uploads/sites/2/2018/10/phising_dt_web.pdf.

Kundinnen und Kunden ist zu empfehlen, die Meldemöglichkeiten für Phishing-E-Mails an reports@antiphishing.ch und Phishing-URL über antiphishing.ch zu nutzen, um damit selbst einen Beitrag zur Erkennung und Vermeidung von Phishing E-Mails zu leisten.

4 Ergänzung von Verträgen bzw. AGB

AGB-Bestimmung zu Anti-Phishing-Massnahmen:
«Der Schutz unserer Kundinnen und Kunden vor möglichen Schäden durch Spam (einschliesslich Phishing-E-Mails, siehe [Link zur Informationsseite der Anbieterin]) ist uns wichtig. Als technische Massnahmen können wir z.B. Filter einsetzen, um verdächtige E-Mails zu identifizieren und abzufangen. Durch das Unterdrücken oder Verschieben von verdächtigen E-Mails reduzieren wir die Risiken für unsere Kundinnen und Kunden. Solche Massnahmen können wir auch auf E-Mails anwenden, die bereits in ihren Posteingang ausgeliefert wurden, nachträglich aber als Phishing-E-Mails erkannt werden. Damit wir Phishing-E-Mails noch besser erkennen, können wir auf geeignete externe Informationsquellen zugreifen. Wir richten uns dabei nach der Branchenempfehlung Phishing-E-Mails des Branchenverbandes Swico.

Damit unsere Massnahmen noch wirksamer sind und die Urheber von Phishing-Versuchen der Strafverfolgung zugeführt werden können behalten wir uns vor, identifizierte Phishing-E-Mails den zuständigen Behörden und Organisationen (z.B. dem NCSC über antiphishing.ch) zu melden. Wir können zur Verbesserung der Filtermassnahmen und zur Strafverfolgung insbesondere verdächtige URL, IP-Adressen des Absender-Servers sowie relevante Merkmale von E-Mail-Headern Dritten (z.B. der SISA, dem NCSC oder der Schweizerischen Strafverfolgungsbehörden) weiterleiten. Soweit möglich, geben wir dabei keine Personendaten bekannt. Die übermittelten Informationen können im Ausnahmefall auch Personendaten (wie Namen, E-Mail-Adressen und personenbezogene E-Mail-Inhalte) umfassen. Personendaten dürfen aber von den Empfängern in jedem Fall nur für den Zweck der Identifikation, Bekämpfung und Verfolgung von Phishing-Versuchen verwendet werden.

Technische Massnahmen gegen Phishing sind nicht fehlerfrei und können E-Mails fälschlicherweise als verdächtig einstufen («false positive») oder Phishing-E-Mails nicht auffinden («false negative»). Wir schliessen jegliche Haftung für entstandene Schäden bzw. den Verlust von Daten im Zusammenhang mit Anti-Phishing-Massnahme aus, sofern nicht grobfahrlässiges oder vorsätzliches Verhalten unsererseits zu einem Schaden geführt hat.»

Für Rückfragen zur Branchenempfehlung:

Giancarlo Palmisani
SWICO
Leiter Verbandsdienstleistungen
Mobile: +41 79 429 53 39 Direkt: +41 44 446 90 85
Mail: Giancarlo.palmisani@swico.ch