

Pressemeldung

Steigende Phishing-Bedrohung zwingt Unternehmen zum Umstellen ihrer Kundenkommunikation

**~ E-Mail-Signatur zwar als Ausweg erkannt, doch laut TC TrustCenter informieren
nur wenige ihre Kunden über neue Wege des sicheren Maildialogs ~**

Hamburg, 21. November 2006 – Die Zahl der Phishing-Angriffe steigt unaufhaltsam: Waren laut der Anti-Phishing Working Group (APWG) im Mai noch knapp 12.000 Phishing-Webseiten online, gab es im Juli schon 14.191 – Tendenz steigend. In Deutschland lagen die dadurch verursachten Schäden bei rund 5 Millionen Euro*. Auffällig ist, dass sowohl die Phishing-Websites als auch die dazugehörigen betrügerischen E-Mails immer professioneller werden und täuschend echt wirken. Als Kommunikationsmittel kann E-Mail daher für bestimmte Branchen wie den Banken- und Finanzsektor mittlerweile kaum noch eingesetzt werden, ohne dass Empfänger an ihrer Echtheit zweifeln. Die Signierung der E-Mails gilt derzeit als sicherste Maßnahme: Laut TC TrustCenter schützen zwar viele Unternehmen bereits ihre Mitarbeiter aktiv vor Phishing, vernachlässigen aber ihre Kunden über die ergriffenen Sicherheitsmaßnahmen zu informieren. Der deutsche Spezialist für digitale Zertifikate und IT-Sicherheitslösungen rät daher jedem Unternehmen, folgende drei goldenen Regeln für die Kundenkommunikation einzuhalten, damit Kunden nicht länger der Eigenverantwortung überlassen sind und der gemeinsame Mail-Verkehr wieder vertrauenswürdig wird.

Folgende drei Schritte sind grundlegend für den Schutz der Kundenkommunikation vor Phishing-Fällen:

- **E-Mail-Signatur als Basisschutz gegen Phishing einsetzen:** Unternehmen sollten ihre E-Mails signieren. Die Schutzvorkehrung kostet nicht viel, verursacht keinen Extraaufwand für Absender und Empfänger und ist dazu noch fälschungssicher. Denn über die Signatur und das dafür eingesetzte Zertifikat kann der Kunde den Absender der E-Mail auf einen Blick überprüfen

und somit zweifelsfrei klären, ob sie echt ist und wirklich von seiner eigenen Bank, Versicherung oder seinem Internetdienstleister stammt.

- **Durch eine offene Kommunikation Vertrauen schaffen:** Unternehmen sollten ihre Kunden umgehend darüber informieren, dass sie in Zukunft ausschließlich signierte E-Mails erhalten und somit alle unsignierten E-Mails nicht von dem vorgegebenen Absender stammen können. Dementsprechend kann der Kunde sein Leseverhalten seines Mailverkehrs umstellen und sich so davor bewahren, Phishing-Mails auf den Leim zu gehen.
- **Durch Aufklärung Kunden die Unsicherheit nehmen:** Schließlich und endlich ist es wichtig, dass das Unternehmen seinen Kunden genau erklärt, was eine signierte E-Mail ist und wie sie diese erkennen können. Dabei kann auch ein Screenshot einer signierten E-Mail oder einer Signatur helfen. Je einfacher der Check verläuft, desto eher sind die Kunden gewillt, die Sicherheitsvorkehrung als Kundenservice anzuerkennen und eventuellen Mehraufwand für höheren Schutz zu akzeptieren.

„Rund 94 Prozent aller Phishing-Mails geben vor, von Finanzunternehmen zu stammen. Der Rest verteilt sich besonders auf Internetdienstleister, Behörden oder Anbieter von Luxusgütern. Der Phantasie der Online-Betrüger sind jedoch keine Grenzen gesetzt“, sagt Dr. Rolf Lindemann, Director Product Management bei TC TrustCenter. „Dementsprechend sollten sich alle Unternehmen zum Ziel setzen, die Interessen ihrer Kunden zu wahren und mit ihnen gemeinsam wirkungsvolle Sicherheitsvorkehrungen zu ergreifen. Nur so können sie langfristig das Vertrauen in die Zusammenarbeit aufrechterhalten sowie ihren eigenen Namen vor Missbrauch und ihre Kunden vor kriminellen Machenschaften schützen.“

TC TrustCenter bietet für Unternehmen jeder Größe verschiedene Zertifikatslösungen als Schutz gegen Phishing an. Informationen zu den einzelnen Lösungen und darüber, wie Unternehmen E-Mailsignatur umsetzen können, sind abrufbar unter <http://www.trustcenter.de>.

*“APWG Phishing Report“ vom Juli 2006 zum Download unter <http://www.antiphishing.org>

Über TC TrustCenter

Die TC TrustCenter GmbH ist einer der führenden Spezialisten für Zertifikate und Sicherheitslösungen entlang der gesamten Wertschöpfungskette von Identity Verification.

Das Portfolio reicht von Web-Sicherheitsdiensten für den Schutz von eCommerce-Transaktionen über Managed Security Services bis zu komplexen PKI Lösungen inklusive umfassender Beratungsdienstleistungen. TC TrustCenter verfügt über mehr als zehn Jahre Erfahrung in nationalen und internationalen Projekten unterschiedlichster Größen und Branchen. TC TrustCenter ist eine gemäß Deutschem Signaturgesetz, Europäischem Signaturgesetz und Identrust akkreditierte Zertifizierungsinstanz.

Unternehmenskontakt TC TrustCenter

GmbH:

Gunilla Pendt
Sonninstrasse 24 - 28
D-20097 Hamburg
Tel.: +49 40 808026-410
Fax: +49 40 808026-126
E-Mail: gunilla.pendt@trustcenter.de
Web: <http://www.trustcenter.de>

Pressekontakt:

LEWIS – Global Public Relations
Marina Ziegler
Baierbrunner Str. 15
D-81379 München
Tel.: +49 89 173019-28
Fax: +49 89 173019-99
E-Mail: marinaz@lewispr.com