

Lösungen gegen »Phishing«

Das Bedrohungspotential von Phishing, speziell im Finanzdienstleistungssektor und im Behördenbereich, ist sehr ernst zu nehmen. Das gilt auch für Österreich.

WIEN – Beim Phishing – so wie jüngstens bei der weltweit erfolgreiche Täuschung von Visa-Kreditkartenkunden – versuchen hochprofessionelle Datendiebe Onlinekunden von Banken, Webshops und Anbietern unterschiedlichster Businessapplikationen mit gefälschten E-Mails auf eine nachgestellte Webseite zu locken, um sie dort zur Eingabe vertraulicher und sensibler Daten zu bewegen und sich so dieser in betrügerischer Absicht zu bemächtigen.

Technisch werden beim Phishing u.a. Sicherheitslücken des marktführenden Internetbrowsers, geringe Awareness der User und Unternehmern gegen diese Form des Datendiebstahls, sowie sicherheitstechnisch nur unzureichend geschützte Businessapplikationen genützt, um an die gewünschten sensiblen persönlichen Userdaten zu gelangen.

Als in Deutschland heuer die ersten Fälle von Phishing öffentlich bekannt wurden war die Aufregung vor allem in der deutschen Banklandschaft groß. Über die finanziellen Schäden dieser modernen Form des Raubritterturns wird beharrlich geschwiegen. Dazu kommt der organisatorische, sicherheitstechnische, logistische und personalintensive Aufwand, um die durch Phishing zugeführten internen Systeme und die IT-Infrastruktur wieder fit zu machen.

Das gilt auch in Österreich. Man erinnere sich nur an gefälschte E-Mails österreichischer Politiker, die tagelang für öffentliche Aufregung und politischen Aufklärungsbedarf sorgten. Während mit solchen Angriffen das wichtigste Kapital eines Politikers, die politische Glaubwürdigkeit, diskreditiert wird, ist der Schaden durch Phishing für heimische Unternehmen neben den erheblichen finanziellen Verlusten vor allem in der nachhaltigen Schädigung des öffentlichen Erscheinungsbildes und der Reputation auszumachen.

AUSWEGE: DNS UND SAUBERUNGSMABNAHMEN

Bei der INTERNET ENGINEERING TASK FORCE (IETF) hat sich Anfang dieses Jahres eine Arbeitsgruppe gebildet, die verschiedene Lösungsansätze verfolgt und zu einem einheitlichen Standard zusammenführen will. Unter dem Sammelbegriff »Sender ID« soll ein einheitliches Vorgehen beschlossen werden, um in Zukunft die Adressaten von E-Mails eindeutig identifizieren zu können. Die Arbeitsgruppe greift dabei sowohl auf Microsofts Lösung Caller ID zurück wie auf das SENDER POLICY FRAMEWORK (SPF) der Firma Pobox.com

sowie auf die SMTP Submitter Extension von Sendmail. So soll verhindert werden, dass Übelmeinende Absenderdaten von Mails fälschen, insbesondere aber die Domännennamen beziehungsweise -ursprünge von Firmen zweckentfremden, um sich so das Vertrauen der Empfänger solcher E-Mails zu erschleichen.

Der Wiener IT-Sicherheitsexperte DI Wolfgang Prentner, Chef der ZT-Prentner-Informatik sieht in den derzeit entstehenden neue Verfahren zur Validierung von Absenderdaten in E-Mails die Möglichkeit, Spam- und Phishingmails nicht nur aufzuspüren und ihnen entgegen zu arbeiten. Jeder technische Vorschlag, der derzeit in der engeren Auswahl steht, beruht auf einer Ergänzung der Einträge von Mailservern im Domain Name System (DNS). Der empfangende Mailserver überprüft bei einer eingehenden Mail, ob diese wirklich vom für diese Absenderadresse zuständigen Mailserver versendet wurde oder von einem anderen. Dafür fragt er den DNS-Server, der für die im from-Feld abgegebene Domäne zuständig ist, ob der sendende Mailserver der Mail ein autorisierter Mailserver dieser Domain ist.

Ein weiterer Lösungsansatz um Phishing einzudämmen, ist die Signatur von E-Mails, wobei der Umgang mit signierten Mails angesichts verschiedener Standards und zahlreicher Clients in der Praxis noch optimiert werden kann. Abgesehen davon sind Signaturen im Bereich der Clients, aber auch speziell im Serverbereich als Lösung denkbar. Mittelfristig wird auch eine grundlegende Änderung des Protokolls von E-Maildiensten zu einer technologischen Weiterentwicklung und damit zu einem besseren Schutz vor Phishing führen.

Vorbereitende Maßnahmen sind im Umgang mit potentiellen Phishing-Angriffen unerlässlich, macht IT-Ziviltchniker Prentner, der auch Mitglied der weltweit agierenden Antiphishing Working Group ist, klar. Dazu gehören kontinuierliche Sicherheitsmaßnahmen in den Unternehmen (moderne und aufeinander abgestimmte IT-, Webserver- und Mailserver-Policies), die Schaffung von erhöhter Aufmerksamkeit im Kundenkreis durch kontinuierliche Kommunikation und der vertrauensvolle Umgang mit sensiblen Userdaten durch das Unternehmen und die Benutzer. Zum Schutz der firmeneigenen Webapplikationen vor cross-site-scripting ist es wesentlich, diese auf dem neuesten Softwarestand zu halten und regelmäßig mit geeigneten Tools nach gefährdeten Codesegmenten in ASP-, PHP- und anderen dynamischen Seiten zu suchen.

Abhängig von der jeweiligen Unternehmensstrategie lässt sich durch ein umfangreiches Assessment und darauf aufbauenden Lösungsvorschlägen ein wirkungsvolles Gesamtkonzept zur Phishing-Problematik erstellen, hält Wolfgang Prentner, fest. [e]

Vorbereitende Maßnahmen sind im Umgang mit potentiellen Phishing-Angriffen unerlässlich. ☛

