audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Phishing Angriffe – Wie kann ich mich und mein Unternehmen schützen?

Zusammenfassung

Phishing, als eine der ältesten Angriffsmethoden im Informationssicherheitsbereich, ist nach wie vor ein zentrales Problem für Unternehmen jeder Größe. Selbst unerfahrene Angreifer können mit dieser Technik Zugriff auf sensible Unternehmenskomponenten erlangen und damit schwerwiegenden Schaden verursachen.

Die Erstellung von fortgeschrittenen Phishing-E-Mails und dazu passenden manipulierten Fake-Websites lässt sich heute mit frei verfügbaren Werkzeugen schnell und einfach realisieren. Damit erreicht ein Großteil der Phishing-E-Mails ein Niveau, welches es sogar erfahrenen Mitarbeitern aus der IT-Abteilung schwer machen kann, jede dieser E-Mails zu durchschauen.

Gleichzeitig steigt das Niveau der technischen Erkennungs- und Filterwerkzeuge der E-Mail-Anbieter nicht mit gleicher Geschwindigkeit. Manuell erstellte Phishing-Kampagnen kann aktuell kein E-Mail-Dienstanbieter (z.B. Google oder Microsoft) erkennen und filtern. Unternehmen müssen sich also auf einem anderen Weg schützen.

Der einzige effektive und effiziente Schutz ist die Sensibilisierung der Mitarbeiter. Nur wenn alle Mitarbeiter ein Mindestmaß an Bewusstsein aufbauen, können Unternehmen das Risiko Phishing-Angriff heute als angemessen behandelt bezeichnen.

Problemstellung

Phishing ist einer der vielen neuen computerbezogenen Begriffe, die in den letzten zehn Jahren Eingang in das allgemeine Lexikon gefunden haben. Seine "ph"-Schreibweise wird durch ein früheres Wort für eine unerlaubte Handlung beeinflusst: "Phreaking". Beim Phreaking wird ein elektronisches Gerät in betrügerischer Absicht benutzt, um das Bezahlen von Telefongesprächen zu umgehen. Beim Phishing wird dagegen nach Benutzerdaten "gefischt".

Angreifer versuchen durch Phishing, den Benutzer zu täuschen und diesen dazu zu bringen, sensible Informationen preiszugeben. Phishing erfolgt typischerweise über elektronische Kommunikationsmittel und beinhaltet Spoofing. Als Spoofing wird das Vortäuschen einer anderen Identität, meist von Banken, Großunternehmen oder staatlichen Institutionen, bezeichnet. Dazu werden sowohl die Nachricht selbst (Absender und Erscheinungsbild) als auch Webseiten, zu denen die Nachricht weiterleitet, der kopierten Entität nachempfunden. Phishing ist eine der ältesten und bekanntesten Angriffsformen in der IT-Sicherheit.

Der klassische Phishing-Angriff wird auch als "Bulk-Phishing" bezeichnet und zielt auf ein möglichst großes Publikum ab. Daher werden häufig generische E-Mails verwendet, welche an eine möglichst große Anzahl potenzieller Opfern gesendet werden kann. Typischerweise beziehen sich diese E-Mails daher auf weit verbreitete Software (z.B. Apple oder Microsoft Produkte) oder auf allgemeine Gewinnspiele. Da viele persönliche Daten digital frei verfügbar sind oder zu einem vorherigen Zeitpunkt bereits kompromittiert worden sind, fügen einige moderne Phishing-Kampagnen persönliche Informationen, wie z.B. Accountnamen automatisch in die E-Mail ein. Trotzdem zielen auch diese E-Mails auf die breite Masse oder z.B. alle Mitarbeiter eines Unternehmens ab.

Laut einer Studie von Trend Micro gehören Phishing-E-Mails weiterhin zu der häufigsten Methode von Cyber-Angriffen. 39 Prozent der befragten Sicherheitsentscheider in Unternehmen aus Deutschland geben an, dass ihre Firma bereits Opfer dieser Art von Angriffen geworden ist. Im Schnitt werden monatlich (!) 78.000 Phishing Seiten identifiziert. Symantec hat in einer Studie festgestellt, dass im Schnitt eine von 323 E-Mails von Angreifern erzeugt wurde. Trend Micro zufolge ist die Anzahl der von ihnen geblockten, bösartigen Phishing-URLs seit 2015 um 2.500 Prozent gestiegen. Laut den Experten von Trend Micro ist diese Angriffsmöglichkeit aufgrund ihres geringen Aufwands in Relation zu ihrem Schaden so beliebt. Grundsätzlich kann jeder (erfolgreiche) Phishing-Angriff katastrophale Folgen für ein Unternehmen haben. Konkret lassen sich diese Folgen jedoch nur schwer quantifizieren, da Phishing zumeist nur das Einfallstor in das interne Unternehmensnetzwerk darstellt. Nutzt der Angreifer nach einer erfolgreichen Phishing-Kampagne z.B. Ransomware (Verschlüsselungstrojaner), um alle Dateien des Unternehmens zu verschlüsseln und anschließend Lösegeld zu verlangen, kann dies die Insolvenz des Unternehmens bedeuten. Aufgrund einer sehr hohen Dunkelziffer existieren keine eindeutigen Zahlen, Experten schätzen jedoch, dass etwa ein Fünftel der von Ransomware betroffenen Unternehmen Insolvenz anmelden muss.

Lösungsansatz

Technische Maßnahmen zur Abwehr von Phishing-Angriffen sind zwar sehr wichtig, werden jedoch von fast allen namenhaften E-Mail-Dienst Anbietern bereits effektiv durchgesetzt. Eine Investition in den Ausbau dieser Maßnahmen bringt nur selten einen nennenswerten Zuwachs an Sicherheit. Viel entscheidender sind daher Maßnahmen auf einer anderen Ebene, zumal durch technische Maßnahmen ohnehin niemals eine 100%tige Sicherheit erreicht werden kann.

Udo Schneider, Security Evangelist bei Trend Micro, sieht vor allem den Menschen als Sicherheitslücke: „Diese Angriffe sind deshalb so erfolgversprechend, da sie die ‚Schwachstelle Mensch' ins Visier nehmen. Um sich wirksam zu schützen, sollten Unternehmen neben einer zeitgemäßen IT-Sicherheitslösung vor allem in die Aufklärung und Schulung ihrer Mitarbeiter investieren." Diese Meinung teilt auch audatis. Nur wenn alle Mitarbeiter ein Mindestmaß an Bewusstsein für die Problemlage aufgebaut haben, können Angriffe in der Praxis abgewehrt werden. Der Mitarbeiter muss aktiv mit realitätsgetreuen Phishing-Angriffen in Kontakt kommen, um im Ernstfall die richtige Entscheidung treffen zu können.

Autor und Ansprechpartner

Marcel Albrink
Consultant Informationssicherheit

Schwerpunkte: IT-Schwachstellenanalyse, Sichere Softwareentwicklung

Mail: m.albrink@audatis.de
Fon: 05221 87292-06
XING **Linkedin**

Haben Sie noch Fragen?

Wir haben versucht alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis Datenschutz und Informationssicherheit | CONSULTING

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de