PRODATIS®

The eBusiness Solution Company.

Phishing-Simulationen: Darauf müssen Sie achten

In den letzten Monaten warnten Sicherheitsbehörden vor Phishing-Wellen im Zusammenhang mit der Covid-19-Pandemie. Schon zuvor war Phishing eine ernstzunehmende Gefahr für den Schutz personenbezogener Daten. Grund genug, eine spezielle Schulung anzubieten. Wer dabei Phishing-Simulationen nutzt, sollte das genau vorbereiten.

Vor Phishing wird gewarnt

Cyberkriminelle verschicken angeblich von Förderbanken stammende Phishing-E-Mails, um an Informationen zu gelangen, warnte das Bundeskriminalamt (BKA) im Mai 2020. Die Angreifer forderten die Empfänger der Mails auf, persönliche Informationen sowie eine Bescheinigung über erhaltene Corona-Soforthilfen an eine E-Mail-Adresse zu übermitteln, die die Täter kontrollierten.

In den Dokumenten, die sie der E-Mail beigefügt hatten, bauten die Täter eine Drohkulisse hinsichtlich der Rückzahlung von erhaltenen Fördergeldern auf.

… auch im Homeoffice!

Diese Phishing-Gefahr besteht weiterhin und ist nur ein Beispiel von vielen. Auch in Verbindung mit der gestiegenen Nutzung von Homeoffice kommt es zu Phishing-Attacken. So erklärte das BSI (Bundesamt für Sicherheit in der Informationstechnik), es könnten vermehrt Phishing-E-Mails auftreten, die die aktuelle Situation ausnutzen und versuchen, sensible Daten mit Hinweis auf Remote-Zugänge, das Zurücksetzen von Passwörtern etc. abzugreifen.

Menschen machen Fehler

Phishing gehört zu den Angriffen, die die sogenannte „Schwachstelle Mensch" ausnutzen. Dazu Arne Schönbohm, Präsident des BSI:

„Menschen machen Fehler, das ist ganz normal. Diese Fehler sollten aber nicht dazu führen, dass Schaden für das Unternehmen entsteht, etwa durch Datenabfluss, Know-how-Diebstahl oder unautorisierte Geldtransfers. Der Faktor Mensch ist deswegen ein wesentlicher Bestandteil jedes nachhaltigen Sicherheitskonzepts."

Es ist deshalb wichtig, auch in der Datenschutz-Schulung regelmäßig zu behandeln, wie die Datendiebe Menschen austricksen und wie die Beschäftigten sich am besten schützen. Zur Aufklärung bieten zum Beispiel das BSI und

die Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) Checklisten und Flyer an.

Beim Thema Phishing kommen bei Schulungen aber auch Simulationen zum Einsatz. Es starten simulierte Phishing-Attacken, um zu sehen, wie die Mitarbeiterinnen und Mitarbeiter als Empfänger der angeblichen Phishing-Mails reagieren.

Phishing-Simulationen gut vorbereiten

Nicht nur die Angreifer können Phishing-Tools nutzen, um ohne großen Aufwand eine Attacke zu starten. Auch für die „gute Seite" gibt es Werkzeuge, die simulierte Angriffe unterstützen.

Auf dem Markt gibt es inzwischen zahlreiche Lösungen, die sogar automatisierte Simulationsangriffe möglich machen. Sie verschicken regelmäßig und ohne großen Aufwand für Security- und Datenschutz-Verantwortliche simulierte Phising-Mails an interne Ziele.

Auch wenn später automatisierte Simulationen möglich sind: Beginnen Sie eine Schulungs-Maßnahme nicht ohne Vorbereitung. Immerhin gilt es, unerwünschte Nebenwirkungen zu vermeiden.

Fallstricke bei Phishing-Simulationen

Ein Bericht des Karlsruher Instituts für Technologie (KIT) und der Ruhr Universität Bochum hat Phishing-Kampagnen unter den Aspekten „Security, Recht und Faktor Mensch" beleuchtet.

„Die Kampagnen haben das Ziel, Mitarbeiterinnen und Mitarbeiter bewusst zu täuschen, um sie vor realen Gefahren zu schützen und ein Problembewusstsein zu schaffen, aber es herrschen oft Unsicherheiten darüber, was rechtlich, sicherheitstechnisch und ethisch vertretbar ist", so der Bericht.

„Phishing-Kampagnen bringen eine Reihe von Sicherheitsproblemen mit sich, und sie beeinflussen die Vertrauens- und Fehlerkultur in einem Unternehmen stark; auch rechtlich ist einiges zu berücksichtigen", sagt Franziska Boehm, die neben ihrer Professur am KIT auch Bereichsleiterin am FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur ist.

Mitarbeitende informieren oder nicht?

„Eine Kampagne zu starten, ohne die Angestellten vorher darüber aufzuklären, ist schlicht unfair und trägt nicht zum Vertrauen in die Leitung bei", sagt die Bochumer Professorin für Human-Centred Security am Horst-Görtz-Institut für IT Sicherheit, M. Angela Sasse.

Zu erfahren, dass man auf Phishing-Nachrichten hereingefallen ist, wirke sich schlecht auf die Selbstwirksamkeit aus: „Die Angestellten merken, dass sie keine Kontrolle über die Situation haben und reagieren mit Resignation, sie bemühen sich nicht einmal mehr, Phishing-Nachrichten zu erkennen", stellen die Autorinnen fest.

Andererseits: Wissen die Mitarbeiter, dass die Kampagne läuft, sind sie vielleicht neugierig und klicken eine Mail an in der Annahme, da könne nichts passieren, die Mail sei ja fingiert. Da aber weiterhin echte Phishing-Mails im Umlauf sind, setze das das Schutzniveau herab, so eine Warnung des Berichts.

Merkt ein Mitarbeiter, dass er doch einen gefährlichen Link angeklickt hat und traut er sich nicht, dies zu melden, verstärkt das das Problem. Unternehmen sollten deshalb eine Meldepflicht von IT-Sicherheitsvorfällen etabliert haben, bevor sie eine Phishing-Kampagne starten, betonen die Autorinnen der Studie.

- Die Studie rät Unternehmen, die ihre IT-Sicherheit stärken wollen, Zeit und Geld in erster Linie zu investieren, um die technischen Sicherheits-Maßnahmen zu verbessern.
- Erst im zweiten Schritt sollten sie die Beschäftigten schulen, welche Phishing-Nachrichten sie trotz der aktuellsten Sicherheits-Software und des neuesten Betriebssystems erreichen können und wie sie diese E-Mails erkennen.

Schulungs-Maßnahmen immer zuerst bewerten

Anbieter entsprechender Simulations-Lösungen sehen dies anders und kommen in ihren Umfragen zu anderen Ergebnissen. Darunter ist auch die Studie „Nutzen und Herausforderungen von Cybersecurity Awareness 2020" des Schweizer Unternehmens Lucy Security AG:

- 73 Prozent der befragten Unternehmen bestätigten demnach, dass die Security-Awareness-Maßnahmen keine Ängste unter den Mitarbeitenden auslösen.
- Ganz im Gegenteil: 95 Prozent der Befragten geben laut Studie an, dass sich die Phishing-Simulationen positiv auf das Betriebsklima auswirken.
- 100 Prozent behaupten zudem, dass die Maßnahmen die Fehlerkultur ihres Unternehmens positiv beeinflussen.

Wichtige Punkte für die Prüfung

Diese unterschiedlichen Studienresultate zeigen, wie wichtig es ist, Schulungs-Maßnahmen immer vorab daraufhin zu prüfen, ob

- Nebenwirkungen möglich sind,
- die Daten der Schulungs-Teilnehmer geschützt sind und
- sich die Ziele mit der Schulung wirklich erreichen lassen.

Ganz ohne Aufwand gibt es eben keine Schulung für mehr Datenschutz – und wenn es die Zeit ist, die Sie in die Prüfung der Schulungs-Methode stecken.

Aber eines ist sicher: Nicht nur die Datenschutz-Grundverordnung (DSGVO) fordert, die Mitarbeiterinnen und Mitarbeiter zu sensibilisieren. Erfahrungsgemäß reichen die technischen Sicherheits-Maßnahmen nicht, um aus der Schwachstelle Mensch die sogenannte Human Firewall zu machen.

Quelle:
www.heise.de