Liebe Leserin, lieber Leser,

diese Ausgabe betrachtet, wie Sie am besten auf die erhöhte Gefahr durch Phishing-Mails reagieren.

Viel Spaß beim Lesen!

Wenn hoher Informationsbedarf zum Risiko wird

Datendiebe nutzen das große Interesse an Informationen zur aktuellen Lage aus, um Zugangsdaten auszuspionieren. Ein Schutz vor Phishing-Mails darf jetzt nicht fehlen.

Vorsicht vor gefälschten Webseiten und Phishing-Mails

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Zunahme von Cyberangriffen mit Bezug zum Coronavirus beobachtet. So werden Unternehmen per E-Mail aufgefordert, persönliche oder unternehmensbezogene Daten auf gefälschten Webseiten preiszugeben. Die Cyberkriminellen geben sich zum Beispiel als vermeintliche Institutionen zur Beantragung von Soforthilfegeldern aus. Die betrügerisch erlangten Daten werden anschließend für kriminelle Aktivitäten missbraucht.

Das erhöhte Informationsbedürfnis im Internet nutzen Cyberkriminelle auch auf anderen Wegen aus. So konnte das BSI eine deutliche Zunahme an Registrierungen von Internetadressen mit Schlagwörtern wie „corona“ oder „covid“ beobachten.

Neben der Nutzung für legitime Informationsangebote werden viele dieser Internetadressen für kriminelle Aktivitäten missbraucht. Nutzer werden auf solchen Webseiten zum Download von Informationen aufgefordert. Tatsächlich infiziert das die Systeme der Nutzer mit Schadprogrammen. Ebenso werden Spam-Mails mit vermeintlichen Informationen in Bezug auf Corona im Dateianhang verschickt, um Schadprogramme zu verbreiten.

Phishing-Attacken nutzen psychologische Tricks

Die Corona-Krise ist dabei nur ein Thema, das Angreifer bei Phishing-Attacken ausnutzen, um die Zugangsdaten der Mail-Empfänger zu erbeuten. Immer wenn sich Menschen für etwas besonders interessieren, besteht für die Angreifer eine größere Chance, für ihre Attacken viele Opfer zu finden.

In einer ernsten Lage werden zudem Vorsichtsmaßnahmen beiseitegelegt, um möglichst schnell an die wichtigen Informationen zu kommen. Wenn man sich um die Gesundheit der Familie oder der Beschäftigten sorgt, scheinen die Bedenken um den Datenschutz nicht nur zweitrangig zu sein, man denkt einfach nicht mehr daran.

Deshalb ist es wichtig, beim Phishing-Schutz auch auf Lösungen zu setzen, die sich nicht mit psychologischen Tricks aushebeln lassen, Lösungen, die automatisiert nach Anzeichen für Mail-Attacken suchen. Deshalb sind jetzt Phishing-Filter wichtig, die lokal im Mail-Programm arbeiten und regelmäßig mit neuen Kennzeichen für Attacken aktualisiert werden.

Phishing-Schutz aus Mensch und Maschine

Jeder Nutzer von digitalen Kommunikationslösungen wie Mail und Chat sollte besonders vorsichtig sein und nicht einfach Links in Mails oder in Suchmaschinen anklicken, sondern die korrekte Internetadresse direkt in den Webbrowser eintippen.

Zusätzlich zu dieser Vorsichtsmaßnahme sollten im Mail-Programm und im Browser die Phishing-Filter aktiviert sein, die Internetadressen gegen bekannte, bösartige Webadressen abgleichen können. Automatisierter Phishing-Schutz und menschliche Awareness sorgen dann gemeinsam für den Datenschutz in Krisenzeiten.

Zusammenfassend die häufigsten Merkmale einer Phishing-Mail:

- Grammatik- und Orthographiefehler

- fehlende persönliche Ansprache (z.B. " Sehr geehrter Kunde")

- dringender Handlungsbedarf (Handeln innerhalb einer kurzen Frist)

- Eingabe von Daten (persönliche Daten, Passwörter, etc.)

- Aufforderung zur Öffnung einer Datei oder zum Klicken auf Links

- Mailabsender (gefälschte Email der Geschäftsleitung)