Text ↦ Patricia Staniek

Giftige Pilze

Die Phising-Technologie bedient sich immer raffinierterer Tricks und Systeme, um an Geldkonten, Geschäftsinformationen oder das geschützte Betriebswissen von Unternehmen heranzukommen. Dabei spielen Myzelien, eingeschleuste Pilz-Netzwerke, eine zunehmend gefährliche Rolle.

Phisher sind kreativ. Sie entwickeln ihre Techniken ständig weiter. Die Pandemie hat ein zusätzliches Wachstumsfeld für Angriffe ermöglicht – das Homeoffice. Mitarbeiter*innen im Homeoffice bekommen mit Schadprogrammen infizierte E-Mails von seriös erscheinenden Absendern wie zum Beispiel Banken, welche auch tatsächlich im Kooperationsverhältnis des Unternehmens stehen. Das passiert oft dann, wenn Mitarbeiter*innen mit ihrer privaten Hard- und Software arbeiten.

Das Ziel ist, an Passwörter und relevante Bankinfos zu kommen. Die Angriffe gehen nicht nur auf Mittelbetriebe und Konzerne, sondern auch gezielt auf Unternehmen, die sich in einer angespannten wirtschaftlichen Situation befinden, weil sie nur wenige finanzielle Mittel für zusätzliche Sicherheitsmaßnahmen einsetzen.

Zunehmend raffinierte Techniken

Sobald der Computer mit der Malware infiziert ist, dient er als „Myzel", als eine Art „Pilz-Netzwerk", das der Verbreitung des Trojaners (= Angreifer) dient. So verbreiten sich diese im Netzwerk, recherchieren gleichzeitig, in welchem Unternehmen sie jetzt „eingecheckt" sind, erkunden dessen Ressourcen und Situation – und legen so das Lösegeld fest, um die Unternehmen zu erpressen. Diese Myzel-Netzwerke sind meist Teil von professionellen Phishingorganisationen.

Attacken passieren aber nicht nur per E-Mail, sondern auch telefonisch. Die Phisher geben sich als legitimierte IT-Mitarbeiter oder externe IT-Dienstleister aus und versuchen, durch Manipulation der Mitarbeitenden Zugriff etwa auf Benutzerwörter, Bankdaten und andere sensible Infos zu erhalten oder Malware zu installieren. Diese Informationen werden verwendet, um auf Unternehmenssysteme zuzugreifen und Identitätsdiebstahl oder Erpressungen durchzuführen. Oder: Die Mitarbeiter*innen der Buchhaltung zahlen unbeabsichtigt Rechnungen auf gefälschte Konten ein.

Mitarbeitende fallen darauf rein, weil mit immer geschickteren Social-Engineering-Techniken manipuliert wird. Sie werden überredet, Dateien zu öffnen, auf Links zu klicken, die zu infizierten oder kopierten Webseiten führen. Der*die Mitarbeiter*in könnte auf eine Bankseite geleitet werden, die genauso aussieht wie jene, auf der er*sie für sein*ihr Unternehmen agiert. Dort gibt er*sie, manipuliert vom Phisher, die Bankdaten ein, während dieser zusieht und gleichzeitig auf der Originalbankseite die Daten eingibt und Abbuchungen durchführt oder das Konto abräumt.

Phishing-E-Mails, -Anrufe, -SMS etc. sind eine ernsthafte Bedrohung für Unternehmen. Diese Angriffe zielen auf die „Schwachstelle Mensch" ab. Setzen Sie vorbeugende Maßnahmen, schulen Sie Ihre Mitarbeiter*innen – eventuell unter Einbeziehung von Fachkräften –, sensibilisieren Sie sie für diese Themen, implementieren Sie Sicherheitsmaßnahmen und Sicherheitsüberprüfungen, um das Risiko zu vermindern. ⊙

Mag. Patricia Staniek, BBA
ist Profilerin, Kriminalanalytikerin und Akademische Expertin für internes Sicherheitsmanagement.

FOTO: MONI FELLNER