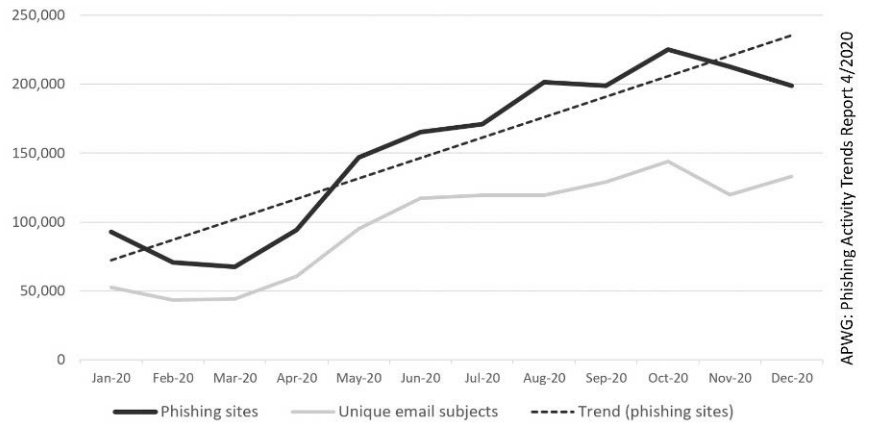
Phishing

Eine der größten Gefährdungen von IT-Infrastrukturen stellen derzeit Phishing-E-Mails dar.

Angriffsversuche mit E-Mails, in denen die Empfänger dazu verleitet werden sollen, gefälschte Webseiten aufzurufen, Anhänge mit Schadsoftware zu öffnen, Credentials preiszugeben oder gar Transaktionen auf ein unbekanntes Konto zu veranlassen, gibt es seit weit über zehn Jahren. Deren Schäden waren lange Zeit allerdings begrenzt: Die Angriffe „skalierten" nicht richtig, denn entweder waren die (meist privaten) Rechner der Opfer für die Angreifer finanziell unergiebig, oder die „Strohmänner", die ihr Konto für ergaunertes, überwiesenes Geld bereithielten und das Geld abhoben, waren rar. Selten hatten die Opfer der Angriffe Verfügungsgewalt über große Geldmengen, von „CEO-Fraud" einmal abgesehen.

Das änderte sich, als findige Kriminelle auf die Idee kamen, anstatt mühsam nach wertvollen Daten zu suchen, einfach alle von einem angegriffenen System erreichbaren Dateien zu verschlüsseln – und den Besitzer (oder das Unternehmen) ein Lösegeld für die Entschlüsselung zahlen zu lassen. Als simple Erpressung sind Ransomware-Angriffe ein finanziell attraktives und zugleich risikoarmes Geschäft: Die Angriffs-Tools kann man „mieten", die Lösegeldzahlungen sind erheblich und dank Bitcoin ist die Chance, unentdeckt davonzukommen, vergleichsweise groß. Zahlreiche Angreifergruppen wurden so bereits zu Millionären – und Ransomware zur weltweit größten (IT-)Schadensursache. Die Zahlen des „Phishing Activity Trends Report 2020" zeigen den rasanten Anstieg dieser Angriffsform allein im vergangenen Jahr.

Abb. 1 | Phishing Aktivitäten 2020



Auf Ransomware-Angriffe kann man sich natürlich vorbereiten – die „üblichen" Schutzmaßnahmen wie regelmäßige Updates, Filterung von E-Mails mit möglichen Schadanhängen und natürlich häufige Backups helfen, das Risiko zu reduzieren. Will man sie wirksam abwehren, muss man allerdings die Mitarbeiterinnen und Mitarbeiter mit ins Boot nehmen: Der Klick auf die Schadsoftware erfolgt schließlich nicht im Rechenzentrum, sondern vor dem Bildschirm. Und das ist gar nicht so einfach, denn wir haben uns daran gewöhnt, dass Phishing-E-Mails leicht zu erkennen sind. Das liegt allerdings daran, dass sie (bisher) meist schlecht gemacht wurden – und damit steigt die Wahrscheinlichkeit, dass Benutzer ihre eigene Resistenz über- und damit die Gefahr unterschätzen. Was Sensibilisierungsmaßnahmen dazu beitragen können, die Erkennung von Phishing-E-Mails zu verbessern, beleuchten wir in diesem Heft.

Dirk Fox