Phishing testen statt nur darüber sprechen

12.10.2026, 10:05 | IT, New Media & Software

Pressemitteilung von: *NetWyl Informatik GmbH*



Phishing lässt sich nicht allein mit Schulungen verhindern. Simulationen zeigen, wie Mitarbeitende in realistischen Situationen reagieren - und wo Security Awareness gezielt verbessert werden kann.

Luzern, Oktober 2026 - Mitarbeitende werden regelmässig vor Phishing gewarnt. Sie lernen, verdächtige Absender zu erkennen, Links zu prüfen und bei ungewöhnlichen Anfragen vorsichtig zu sein. Trotzdem bleibt eine zentrale Frage häufig unbeantwortet: Wie reagieren sie tatsächlich, wenn eine täuschend echte Nachricht während eines hektischen Arbeitstags im Posteingang landet?

Genau hier setzen Phishing-Simulationen an. Sie ersetzen klassische Awareness-Schulungen nicht, sondern machen sichtbar, was theoretische Schulungen allein kaum zeigen können: wie Menschen unter realistischen Bedingungen auf digitale Täuschungsversuche reagieren. NetWyl Informatik aus Luzern setzt dabei auf individuell entwickelte Szenarien, messbare Ergebnisse und einen Ansatz, bei dem nicht einzelne Mitarbeitende blossgestellt, sondern Sicherheitslücken systematisch erkannt und bearbeitet werden.

Wenn eine Phishing-Mail nicht wie eine Phishing-Mail aussieht

Eine verdächtige Nachricht mit offensichtlichen Rechtschreibfehlern und einer unbekannten Absenderadresse ist vergleichsweise leicht zu erkennen. Schwieriger wird es, wenn eine Nachricht genau dort ansetzt, wo Mitarbeitende täglich kommunizieren.

Eine angebliche Nachricht der Personalabteilung. Eine Aufforderung, ein Microsoft-365-Konto zu bestätigen. Eine Information über eine bevorstehende Paketlieferung. Eine neue Rechnung eines bekannten Lieferanten. Oder eine kurzfristige Anfrage der Geschäftsleitung.

Solche Situationen sind im Arbeitsalltag nicht ungewöhnlich. Genau deshalb können sie als Grundlage für Phishing-Angriffe dienen. Moderne Kampagnen orientieren sich zunehmend an bekannten Abläufen, Rollen und Kommunikationsmustern. NetWyl beschreibt in seinem aktuellen Fachbeitrag, dass insbesondere Nachrichten zu Rechnungen, Cloud-Diensten, Login-Problemen, Dokumentfreigaben oder internen Anfragen genutzt werden können, um Vertrauen auszunutzen.

Das Problem ist dabei nicht zwingend mangelndes Wissen. Ein Mitarbeitender kann sehr wohl wissen, dass Phishing existiert - und trotzdem in einer konkreten Situation auf einen Link klicken.

Lesen Sie mehr zum Thema Phishing auf der Seite der Netwyl Informatik GmbH: https://www.netwyl-informatik.ch/leistungen/phishing-simulationen/

Wissen und Verhalten sind zwei verschiedene Dinge

Klassische Security-Awareness-Schulungen vermitteln wichtige Grundlagen. Mitarbeitende lernen, woran Phishing erkannt werden kann und welche Regeln im Umgang mit E-Mails gelten.

Doch zwischen einer Schulung und dem nächsten tatsächlichen Angriff liegen Wochen oder Monate. Im Alltag kommen Zeitdruck, Routine und zahlreiche andere Aufgaben hinzu.

Eine Phishing-Simulation setzt deshalb an einem anderen Punkt an. Sie stellt keine theoretische Frage wie "Würden Sie auf einen verdächtigen Link klicken?", sondern erzeugt eine kontrollierte Situation, in der sich das tatsächliche Verhalten beobachten lässt.

NetWyl formuliert das auf seiner Phishing-Simulation-Seite bewusst zugespitzt: Schulungen allein reichen nicht aus. Entscheidend sei, wie Menschen im Alltag reagieren.

Das Ergebnis ist nicht als Prüfung einzelner Personen gedacht. Vielmehr entsteht ein Bild davon, wo ein Unternehmen insgesamt steht.

Der Klick ist nur eine Kennzahl

Eine Phishing-Simulation lässt sich auf den ersten Blick auf eine einfache Frage reduzieren: Wer hat geklickt?

Für die Sicherheitsarbeit greift diese Betrachtung allerdings zu kurz.

Ebenso interessant kann sein, wie viele Empfänger eine Nachricht als verdächtig melden, wie schnell eine Kampagne erkannt wird oder ob sich das Verhalten nach einer Schulung verändert. Auch Unterschiede zwischen Abteilungen oder Funktionen können Hinweise liefern.

NetWyl setzt deshalb auf Reports mit konkreten Kennzahlen und Vorher-/Nachher-Vergleichen. Die Ergebnisse sollen nicht lediglich dokumentieren, dass eine bestimmte Anzahl von Personen auf einen Link geklickt hat. Sie sollen eine Grundlage dafür schaffen, gezielte Massnahmen abzuleiten.

Damit wird aus einem einmaligen Test ein Instrument für die kontinuierliche Verbesserung.

Warum Standard-Testmails oft zu wenig aussagen

Eine Testmail, die offensichtlich wie eine Testmail aussieht, liefert nur begrenzte Erkenntnisse.

Wenn ein Unternehmen beispielsweise regelmässig standardisierte Nachrichten mit typischen Phishing-Merkmalen verschickt, lernen Mitarbeitende möglicherweise schnell, genau diese Muster zu erkennen. Das bedeutet jedoch nicht automatisch, dass sie einen realistischeren Angriff erkennen würden.

NetWyl verfolgt deshalb einen anderen Ansatz. Die Kampagnen sollen sich an der tatsächlichen Arbeitswelt des jeweiligen Unternehmens orientieren. Dazu können unter anderem interne Kommunikationsmuster, verwendete Tools, Lieferanten oder typische Geschäftsprozesse berücksichtigt werden. Als mögliche Szenarien nennt NetWyl

beispielsweise HR-Ankündigungen, Paketbenachrichtigungen, Lieferantenwechsel oder CEO-Fraud.

Gerade diese Nähe zum Alltag macht die Simulation aussagekräftiger.

Wenn ein Unternehmen beispielsweise regelmässig mit externen Lieferanten kommuniziert, kann ein Szenario aus diesem Umfeld deutlich relevanter sein als eine generische Testmail. Das Gleiche gilt für HR, Finanzen, Einkauf, Vertrieb oder die Geschäftsleitung.

Nicht der Mitarbeitende ist das Problem

Bei Phishing-Simulationen besteht ein sensibles Thema: Niemand möchte, dass Mitarbeitende das Gefühl bekommen, heimlich geprüft oder an den Pranger gestellt zu werden.

Das kann den Lerneffekt sogar beeinträchtigen.

NetWyl stellt deshalb ausdrücklich den Lerncharakter in den Vordergrund. Die Auswertung kann auf Wunsch anonymisiert werden und beispielsweise nach Teams oder Funktionen erfolgen. Das Ziel sei nicht die Blossstellung einzelner Personen, sondern die Identifikation von Bereichen, in denen zusätzlicher Trainingsbedarf besteht.

Diese Perspektive verändert auch die Interpretation der Ergebnisse.

Eine hohe Klickrate ist nicht einfach eine Liste von Personen, die "Fehler gemacht" haben. Sie kann ein Hinweis darauf sein, dass ein bestimmtes Szenario besonders überzeugend war, eine Abteilung stärker sensibilisiert werden sollte oder bestehende Prozesse angepasst werden müssen.

Umgekehrt ist eine niedrige Klickrate ebenfalls nicht automatisch ein Beweis für umfassende Sicherheit. Entscheidend ist, wie sich das Verhalten über mehrere Tests entwickelt.

Phishing-Simulation als Sicherheitsmessung

Für Unternehmen entsteht dadurch eine zusätzliche Möglichkeit, Security Awareness messbarer zu machen.

Technische Sicherheitslösungen liefern beispielsweise Informationen über blockierte Nachrichten, erkannte Schadsoftware oder verdächtige Aktivitäten. Eine Simulation kann ergänzend zeigen, wie die menschliche Komponente funktioniert.

Das ist besonders relevant, weil Phishing nicht ausschliesslich ein E-Mail-Problem ist. Angriffe können über manipulierte Login-Seiten, gefälschte Dokumentfreigaben, Chat-Nachrichten oder andere digitale Kommunikationswege erfolgen. NetWyl beschreibt moderne Phishing-Angriffe entsprechend als Kombination aus technischer Täuschung und Social Engineering.

Eine Simulation kann deshalb auch dazu beitragen, Sicherheitsbewusstsein über das einzelne E-Mail-Postfach hinaus zu entwickeln.

Melden muss genauso einfach sein wie Klicken

Eine Phishing-Simulation zeigt nicht nur, wer auf eine Nachricht reagiert. Ebenso wichtig ist die Frage, was Mitarbeitende mit einer verdächtigen E-Mail tun. Gibt es einen klaren und einfachen Meldeweg, steigt die Wahrscheinlichkeit, dass verdächtige Nachrichten frühzeitig erkannt und weitergeleitet werden. Unternehmen sollten deshalb neben Schulungen auch die Prozesse rund um Meldungen prüfen. Eine gut sichtbare Anlaufstelle, klare Zuständigkeiten und kurze Wege können dazu beitragen, dass aus einem einzelnen Verdacht schneller eine verwertbare

Sicherheitsinformation wird. So wird Aufmerksamkeit im Alltag tatsächlich nutzbar.

Was passiert nach dem Klick?

Der eigentliche Wert einer Phishing-Simulation zeigt sich nach der Kampagne.

Wenn beispielsweise eine bestimmte Gruppe besonders häufig auf ein Szenario reagiert, stellt sich die nächste Frage: Warum?

Fehlt Wissen über einen bestimmten Angriffstyp? Ist eine Nachricht aufgrund eines realen Geschäftsprozesses besonders glaubwürdig? Gibt es keine klaren internen Regeln für verdächtige Nachrichten? Wissen Mitarbeitende, an wen sie eine verdächtige E-Mail melden sollen?

Aus den Antworten lassen sich konkrete Massnahmen ableiten.

NetWyl beschreibt deshalb einen Ablauf aus Kick-off, Kampagnendesign, Durchführung, Report und Debriefing. Anschliessend sollen die Ergebnisse genutzt werden, um Schulungen oder weitere Sicherheitsmassnahmen gezielt nachzuschärfen. Regelmässige Tests können zusätzlich Veränderungen über einen längeren Zeitraum sichtbar machen.

Ein Test ist kein einmaliges Schulungsprojekt

Security Awareness lässt sich nur schwer mit einer einzigen Schulung dauerhaft herstellen. Arbeitsabläufe verändern sich, neue Mitarbeitende kommen hinzu und Angriffsmethoden entwickeln sich weiter.

Auch die eigenen Kommunikationsgewohnheiten eines Unternehmens verändern sich.
Was heute realistisch wirkt, kann in einem Jahr bereits offensichtlich sein. Gleichzeitig entstehen neue Angriffsmöglichkeiten durch Cloud-Dienste, digitale Freigabeprozesse und zunehmend personalisierte Kommunikation.

NetWyl empfiehlt deshalb wiederkehrende Phishing-Simulationen und bietet neben einmaligen Quick-Checks auch fortlaufende Programme mit quartalsweisen Kampagnen und Trendberichten an.

Der Vorteil liegt dabei weniger im einzelnen Test als in der Entwicklung über die Zeit: Wird die Erkennungsleistung besser? Werden verdächtige Nachrichten häufiger gemeldet? Welche Abteilungen benötigen weiterhin Aufmerksamkeit?

Damit kann Security Awareness von einer einmaligen Schulungsmassnahme zu einem kontinuierlichen Prozess werden.

Technischer Schutz und menschliche Aufmerksamkeit gehören zusammen

Eine Phishing-Simulation ist kein Ersatz für technische Schutzmassnahmen.

E-Mail-Security kann gefährliche Nachrichten erkennen und blockieren. Endpoint Security kann verdächtige Aktivitäten auf Geräten überwachen. Multi-Faktor-Authentifizierung kann die Auswirkungen kompromittierter Zugangsdaten begrenzen.

Trotzdem bleibt der Mensch Teil der Sicherheitskette.

Genau deshalb betrachtet NetWyl Phishing-Simulationen als Ergänzung zu anderen Security-Massnahmen. Auf der Unternehmenswebsite wird der Ansatz als Kombination aus technischer IT-Security, persönlicher Betreuung und laufendem sicheren Betrieb beschrieben.

Piotr Kusak von Wyl, Gründer von NetWyl Informatik, beschreibt den übergeordneten Anspruch so: "Wir sorgen mit massgeschneiderter IT-Security und persönlicher Betreuung für eine sichere Basis, damit Ihr Unternehmen sorgenfrei wachsen und innovieren kann."

Bei Phishing-Simulationen bedeutet das konkret: Nicht nur davon ausgehen, dass Mitarbeitende wissen, wie ein Angriff aussieht, sondern überprüfen, wie sie in einer realistischen Situation tatsächlich reagieren.

Was Unternehmen aus einer Simulation lernen können

Für Unternehmen stellt sich deshalb nicht nur die Frage, ob Mitarbeitende eine Testmail erkennen.
Interessanter sind weiterführende Fragen:

- Welche Angriffsszenarien funktionieren in der eigenen Organisation besonders gut?
- Welche Abteilungen oder Funktionen benötigen zusätzliche Sensibilisierung?
- Werden verdächtige Nachrichten tatsächlich gemeldet?
- Wie verändert sich das Verhalten nach gezielten Schulungsmassnahmen?
- Sind interne Meldewege klar und bekannt?
- Welche technischen Schutzmassnahmen sollten aufgrund der Ergebnisse ergänzt oder angepasst werden?

Eine gute Simulation liefert darauf keine pauschalen Antworten. Sie liefert Daten aus der eigenen Organisation.

Genau darin liegt ihr praktischer Wert.

Testen statt annehmen

Unternehmen können heute vieles über ihre technische Sicherheitslage messen. Bei der menschlichen Komponente bleibt dagegen häufig eine Lücke: Man geht davon aus, dass Mitarbeitende Phishing erkennen, weil sie einmal entsprechend geschult wurden.

Eine kontrollierte Simulation ersetzt diese Annahme durch eine konkrete Beobachtung.
Dabei geht es nicht darum, möglichst viele Klicks zu produzieren oder Mitarbeitende zu verunsichern. Entscheidend ist vielmehr, realistische Situationen zu schaffen, Ergebnisse sachlich auszuwerten und daraus konkrete Verbesserungen abzuleiten.

Phishing-Simulationen werden damit zu einem Werkzeug, das zwischen Schulung und technischer IT-Security ansetzt. Sie zeigen, wo theoretisches Wissen im Arbeitsalltag bereits funktioniert - und wo noch nachgeschärft werden sollte.

NetWyl Informatik verbindet diesen Ansatz mit individuell entwickelten Kampagnen, messbaren Ergebnissen und auf Wunsch regelmässigen Tests. Der Einstieg kann dabei über einen einmaligen Quick-Check erfolgen; für Unternehmen, die ihre Entwicklung kontinuierlich beobachten möchten, sind auch fortlaufende Kampagnen vorgesehen.

Kontaktieren Sie die Netwyl Informatik GmbH: https://www.netwyl-informatik.ch/kontakt/

NetWyl Informatik GmbH

Täschmattstrasse 19
6015 Luzern

PiotrKusak von Wyl

+41 41 520 07 40

piotr.kusak@netwyl-informatik.ch

www.netwyl-informatik.ch

Portrait

Die NetWyl Informatik GmbH mit Sitz in Luzern ist ein spezialisierter Schweizer IT-Dienstleister für Cybersecurity und Netzwerklösungen. Das Unternehmen unterstützt KMU sowie größere Organisationen bei der Absicherung ihrer IT-Infrastrukturen durch maßgeschneiderte Sicherheitskonzepte, Managed Security Services, E-Mail-Security, Cloud-Lösungen und Sicherheitsanalysen. NetWyl kombiniert langjährige IT-Security-Expertise mit persönlicher Beratung und verfolgt das Ziel, Unternehmen zuverlässig vor Cyberrisiken zu schützen und einen sicheren, stabilen IT-Betrieb zu gewährleisten.

News-ID: 1326432 • Views: 65 (Stand: 02.11.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1326432/Phishing-testen-statt-nur-darueber-sprechen.html