Gefördert durch den Strategiefonds #9

Klicken oder nicht klicken, das ist hier die Frage

Die Forschungsgruppe SECUSO untersucht, wie Schulungen für Cybersicherheit effektiv gestaltet werden können. Die Ergebnisse nutzt bereits eine Reihe von Hochschulen und Behörden und bald auch das KIT selbst.

Rund die Hälfte der deutschen Unternehmen ist bereits Opfer von Cyberattacken geworden. 25 Prozent erlitten innerhalb der letzten 12 Monate Schäden durch „Phishing". So heißen Angriffe, bei denen versucht wird, an vertrauliche Daten wie Kennwörter und persönliche Informationen zu gelangen oder Schadsoftware zu verteilen. Solche Schadsoftware ist beispielsweise in der Lage, Computerdaten so zu verschlüsseln, dass selbst Fachleute keinen Zugriff mehr darauf haben. Institutionen und Privatleute können damit erpresst werden, indem für die Entschlüsselung Geld verlangt wird. Im vergangenen Jahr verursachten Datendiebstähle, Industriespionagen und Erpressungen allein in Deutschland einen Gesamtschaden von über 200 Milliarden Euro.

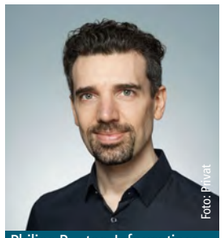


Foto: Privat

Philipp Bunten, Informationssicherheitsbeauftragter des KIT

Auch die IT-Infrastruktur des KIT ist ständig Cyberangriffen unterschiedlichster Art ausgesetzt. Alle der rund 10 000 Mitarbeitenden und knapp 23 000 Studierenden haben ein E-Mail-Konto vom KIT. „Alle E-Mail-Adressen des KIT sind potenzielle Ziele von Cyberattacken", gibt der Informationssicherheitsbeauftragte (ISB) des KIT, Philipp Bunten, zu bedenken. „Die technischen Schutzmaßnahmen werden stetig verbessert, aber die Angriffe leider auch. Daher ist es wichtig, dass wir alle die Risiken von Phishing kennen und entsprechende Sicherheitsmaßnahmen anwenden."

Das Sicherheitsbewusstsein, die Security Awareness, wurde bislang mithilfe von Aktionstagen, Infomails und Webseiten thematisiert. Während der Pandemie fand an den Aktionstagen eine freiwillige Onlineveranstaltung statt. Doch erfolgreiche Cyberattacken an anderen Hochschulen haben gezeigt, dass ein sehr hohes Level an Informationssicherheit notwendig ist, um sich angemessen abzusichern. Da die Bedrohung weiter steigt und die bisherigen Maßnahmen die große Masse noch nicht erreichen, wird nun eine Onlineschulung am KIT etabliert, die zukünftig verpflichtend werden soll.

Der Strategiefond des Präsidiums fördert die Entwicklung dieser Maßnahmen. Verantwortlich sind die Forschungsgruppe SECUSO sowie der Informationssicherheitsbeauftragte des KIT (ISB) und das SCC, insbesondere die Abteilung IT-Security und Service-Management sowie KIT-CERT, mit Unterstützung des IT-Expertinnen- und Expertenkreises.

Foto: Amadeus Bramsiepe

Melanie Volkamer, Leiterin der Forschungsgruppe SECUSO am AIFB

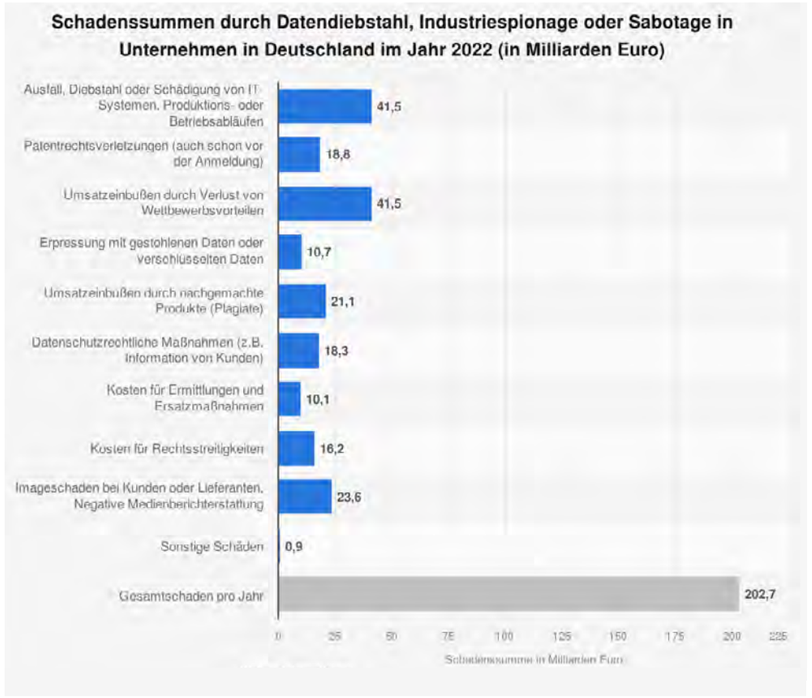
„Inhalte der geplanten 30- bis 45-minütigen Schulungsmaßnahmen werden nach aktuellem Stand ein allgemeiner Überblick über Ansprechpersonen und relevante Dokumente sein", verrät Melanie Volkamer vom Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB), „des Weiteren eine Sensibilisierung für allgemeine Security-Gefahren am Arbeitsplatz und wie diesen begegnet werden kann, sowie das Thema E-Mail-Sicherheit, sprich: Phishing."

Anders als Security-Schulungen von diversen Consulting-Firmen, evaluiert SECUSO den Erfolg der Maßnahmen selbst.

Wer die Qualität der Schulungen verbessern möchte, kann folgende Mailingliste abonnieren, um über Möglichkeiten zur Teilnahme an Feedback-Runden informiert zu werden: **lists.kit.edu/sympa/info/secawareness**

Text: Martin Grolms

Der Strategiefonds des Präsidiums unterstützt Projekte in einem frühen Stadium, für die aus anderen Finanzierungsquellen noch keine Mittel zur Verfügung stehen. Die maximale Fördersumme beträgt bis zu 2,5 Millionen Euro pro Einzelmaßnahme. Das Präsidium möchte damit die strategische Weiterentwicklung des KIT vorantreiben und neue Akzente in Forschung, Lehre und Innovation setzen. Wesentliche Auswahlkriterien für eine Bewilligung sind die Bedeutung für die strategische Ausrichtung und Weiterentwicklung des KIT und die wissenschaftliche Qualität. Die Projekte werden zeitlich befristet gefördert. Es können Personal-, Sach- und Investitionsmittel zur Verfügung gestellt werden. Die Anträge können über die Bereichsleitungen oder über das Präsidium bei der DE Strategische Entwicklung und Kommunikation (SEK) eingereicht werden. Über die Förderung entscheidet in der Regel zweimal jährlich das Präsidium.
Kontakt:
SEK – Strategisches Controlling und Reporting
Tobias Jordan – Tel: - 41135
E-Mail: tobias.jordan@kit.edu



Quelle: Statista / Bitkom

Sei kein Fisch!

Kriminelle Personen versuchen mit Phishing-Mails Konten zu plündern oder Schadsoftware zu installieren. Die Forschungsgruppe SECUSO vom KIT hat eine leicht nachvollziehbare Strategie entwickelt, wie auch Laien eine betrügerische E-Mail sicher erkennen können.

„Der Wurm muss dem Fisch schmecken, und nicht dem Angler" heißt eine einleuchtende, altbekannte Regel. Die meisten Anglerinnen und Angler wissen sehr gut, welchen Köder sie auswerfen müssen, damit Fische anbeißen. Aber nicht nur Menschen, die gerne angeln, kennen sich gut mit Ködern aus. Auch kriminelle Hackerinnen und Hacker wissen, wie sie Beute machen können, und zwar mit Phishing.

Phishing nennen es Fachleute, wenn jemand versucht, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner auszugeben. Der Begriff ist ein englisches Kunstwort, das sich aus password (Passwort) und fishing (Angeln, Fischen) zusammensetzt. Es meint also das Angeln nach Passwörtern mit Ködern – wobei inzwischen neben Passwörtern auch andere sensible Daten abgegriffen oder mittels Phishing Computerviren verteilt werden. Wir, die arglosen Internetnutzenden sind demnach die Fische und die gefälschten E-Mails sind unsere Köder.

„Sehr geehrter Kunde" – in der Regel beginnt eine Phishing-Nachricht mit einer persönlich gehaltenen, offiziell wirkenden E-Mail. Über einen Link sollen wir eine betrügerische Webseite besuchen, die entweder direkt versucht, Computerviren zu installieren oder die mehr oder weniger täuschend

Foto: Daryoush Djawadi

echt aussieht und uns dazu lockt, persönliche Zugangsdaten einzugeben. Ziel des Betrugs kann es auch sein, uns dazu zu verleiten, eine andere schädliche Aktion auszuführen, zum Beispiel eine Überweisung oder einen kostenpflichtigen Anruf zu tätigen.

Die Betrügerinnen und Betrüger können dann unser Konto plündern, unseren Namen für weitere Cyberattacken oder Onlineshopping missbrauchen oder Geld von uns fordern, um die Viren auf dem Computer wieder zu entfernen.

NoPhish-Konzept der Forschungsgruppe SECUSO

„Kriminelle im Internet haben verschiedene Strategien, um Internetnutzende und Unternehmen zu schaden“, sagt Fabian Ballreich, wissenschaftlicher Mitarbeiter der SECUSO-Gruppe. „Die Forschungsgruppe SECUSO am KIT hat daher das NoPhish-Konzept entwickelt, wie jede und jeder ganz einfach betrügerische E-Mails oder andere Nachrichten erkennt.“ Das Konzept umfasst vier Themenbereiche: 1. Einführung in das Thema, 2. Erkennen von unplausiblen, betrügerischen Nachrichten, 3. Erkennen von Nachrichten mit gefährlichen Links und 4. Erkennen von Nachrichten mit gefährlichen Anhängen. „Das NoPhish-Konzept haben wir in unterschiedliche Maßnahmen umgesetzt“, erklärt Melanie Volkamer vom Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB). „Es gibt eine Infokarte mit den wichtigsten Regeln im Hosentaschen-Format oder Flyer, Poster zum Aufhängen im Büro und Videos mit anschaulichen Beispielen.“ Besonders gut kommt neben den Videos (https://s.kit.edu/hm45j1jx) das Quiz Erkennen betrügerischer Nachrichten (https://s.kit.edu/zk4zihk1) an, genauso wie das Onlinespiel Phishing Master (https://s.kit.edu/0z2zyjjk). „Wir haben mit STAR sogar einen humanoiden Roboter, der betrügerische Nachrichten interaktiv mit den Nutzenden bespricht“, sagt Volkamer.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt sogar die Maßnahmen des KIT Konzepts. Bereits 13 andere Hochschulen sowie eine Reihe von Behörden wie etwa das Bundeskanzleramt und das Bundesverwaltungsamt nutzen die Forschungsergebnisse der SECUSO-Gruppe. „Die verschiedenen Maßnahmen sowie das Konzept selbst werden nach wie vor weiterentwickelt, evaluiert und so ständig verbessert“, berichtet Ballreich. Außerdem werden derzeit neue Maßnahmen erarbeitet – etwa ein Kartenspiel und eine Anwendung für einen Touchtable.

Text: Martin Grolms

Foto: Deutsche Stiftung Verbraucherschutz

Für ihre Tools und Tipps zur Privatsphäre im Netz und Cybersicherheit hat die Forschungsgruppe SECUSO den Bundespreis Verbraucherschutz der Deutschen Stiftung Verbraucherschutz (DSV) erhalten. Verliehen wurde der Preis für die Entwicklung nutzungsfreundlicher und einfacher Konzepte und Tools, die Anwenderinnen und Anwender von Online-Diensten, Apps und Software helfen, ihre Privatsphäre und Datensicherheit zu wahren. Mit dem Preis zeichnet die Stiftung des Verbraucherzentrale Bundesverbands herausragende Verbraucherschutz-Projekte aus. (links: Bundesverbraucherschutzministerin Steffi Lemke; rechts: Peter Mayer von SECUSO)

NoPhish – das Security Awareness-Konzept zu Phishing und anderen betrügerische Nachrichten

Folgende sieben Regeln helfen Ihnen, betrügerische Nachrichten zu erkennen:

1. Regel:
Prüfen Sie Absenderadresse und Inhalt jeder Nachricht auf Plausibilität.
✓ Absender info@secuso.org bei einer SECUSO-E-Mail
× Absender info@sye.jp bei einer SECUSO-E-Mail

2. Regel:
Machen Sie sich damit vertraut, wo Sie die tatsächliche Webadresse hinter einem Link finden (zum Beispiel am PC oder Laptop im Tooltip oder in der Statusleiste).

3. Regel:
Identifizieren Sie den Wer-Bereich.
https://nophish.secuso.org/login

4. Regel:
Prüfen Sie, ob der Wer-Bereich zur (vermeintlich) legitimen Nachricht passt und prüfen Sie, ob der Wer-Bereich korrekt geschrieben ist.
✓ https://www.mein-paketservice.de/
× https://s-o-k.de/sicher
× https://www.mein-paketservice.de.shoppen-im-web.de/
× https://shoppen-im-web.de/mein-paketservice.de/
× https://129.13.152.9/mein-paketservice.de/
× https://mein-paketservice.de.s-o-k.de/login
× https://www.bauernmarkt-total.de/
× https://www.baurenmarkt-total.de/
× https://bauemmarkt-total.de/
× https://bauerrnmarkt-total.de/

5. Regel:
Wenn Sie den Wer-Bereich nicht eindeutig beurteilen können, sollten Sie weitere Informationen einholen, z. B. mit einer Suchmaschine.
✓ https://www.secuso.org/
× https://www.secuso-research.org/

6. Regel:
Prüfen Sie das Dateiformat des Anhangs.
× Ausführbare Formate, z. B. .exe, .bat, .cmd
× Dateien mit Makros, z. B. Office-Dateien wie .doc, .docx, .docm

7. Regel:
Wenn Sie den Anhang nicht eindeutig beurteilen können oder unsicher sind, ob Sie genau dieses Format von der Empfängerin oder dem Empfänger erwarten, sollten Sie weitere Informationen einholen, beispielsweise mittels Kontaktaufnahme. Nutzen Sie dafür nicht die Kontaktdaten aus der Nachricht.

So ist ein Link aufgebaut: https://beispiel.kit.edu/news

https:// = Übertragungsprotokoll
beispiel = Subdomain
kit.edu = Die Domain, ein anderer Name dafür lautet „Wer-Bereich“, mit der Top-Level-Domain, was häufig das Länderkürzel wie .de oder .fr ist oder wie hier .edu für eine Bildungseinrichtung
/news = Der Verzeichnispfad, der zu einer bestimmten Datei führt