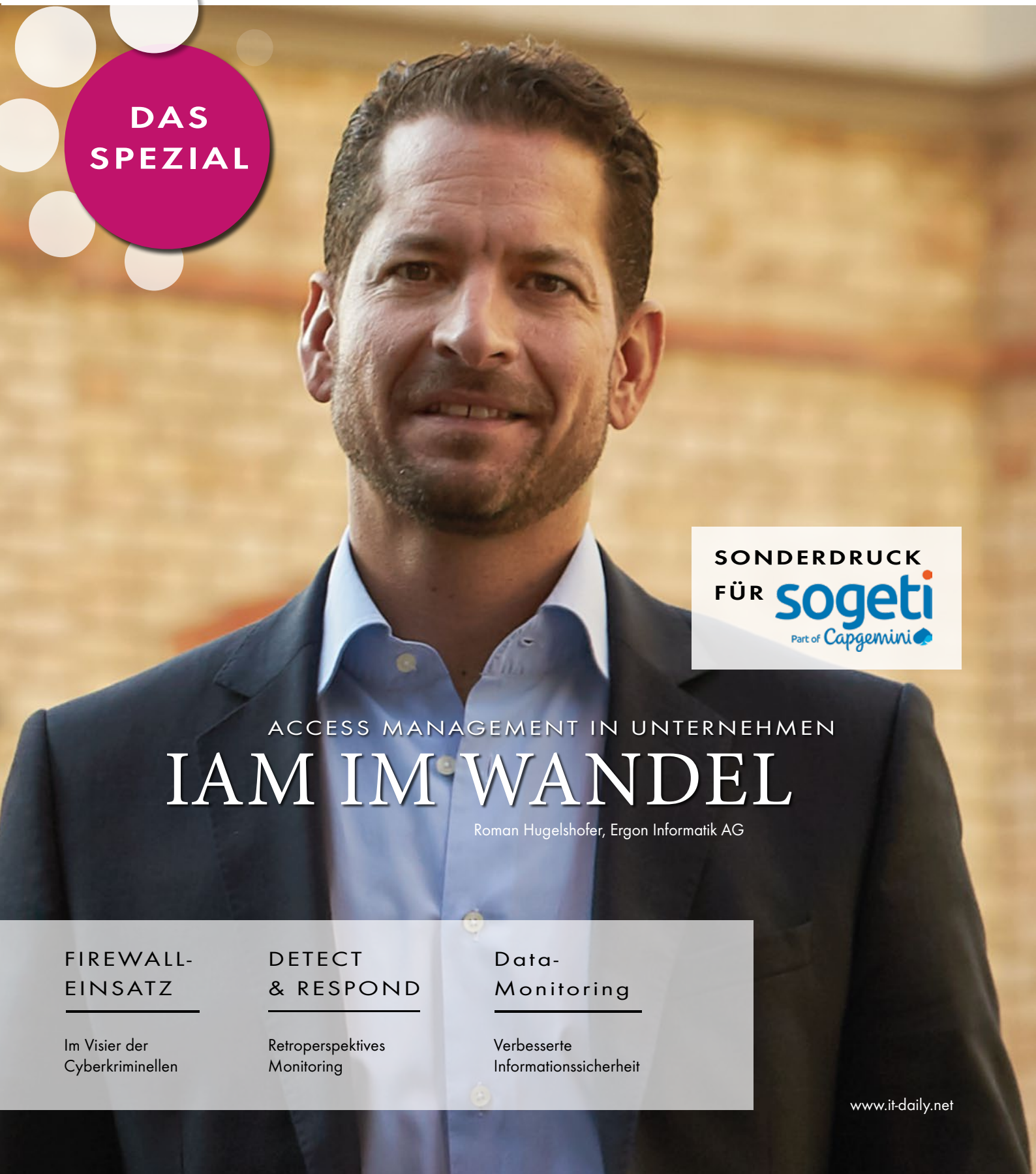
itsecurity
JULI/AUGUST 2019

DAS SPEZIAL



SONDERDRUCK FÜR sogeti Part of Capgemini

ACCESS MANAGEMENT IN UNTERNEHMEN

IAM IM WANDEL

Roman Hugelshofer, Ergon Informatik AG

FIREWALL-EINSATZ
Im Visier der Cyberkriminellen

DETECT & RESPOND
Retroperspektives Monitoring

Data-Monitoring
Verbesserte Informationssicherheit

www.it-daily.net

CYBERSECURITY: AUCH

PHISHING-ATTACKEN WIRKSAM VORBEUGEN.

Jeder war schon einmal Ziel einer Phishing-Attacke. Wir alle sind davon betroffen, dennoch werden Hintergründe und Möglichkeiten dieser Angriffe selten thematisiert. Grob: Phishing ist eine Unterart des Social Engineering. Nicht ein bestimmter Server, ein bestimmtes System, eine bestimmte Software wird angegriffen, sondern die Komponente hinter Server, System und Software: der Mensch.

Physische und digitale Angriffe

Social-Engineering-Angriffe sind nicht zwingend auf die digitale Welt beschränkt, sondern können in Mischformen auftreten, bei denen ein Teil des Angriffs auf physischer Ebene abläuft und ein Teil virtuell, oder sogar als komplett physischer Angriff. Dies lässt sich einfach an einem Beispiel festmachen: wenn ein Angreifer Kreditkartendaten online abgreift und damit einen Flug auf die Malediven bucht, ist der Angriff zwar digital, aber der Betrug physisch. Dennoch ist wichtig zu betonen, dass dies nur eine Art des Phishings ist.

In der Regel hat der durchschnittliche Internetnutzer mit einer simplen Art des Phishing zu tun: Merkwürdige Rechnungen von Firmen, von denen Sie noch nie gehört haben, reihen sich neben EC-Karten-Sperrmails von Banken, bei denen Sie kein Kunde sind – und landen, wenn Sie Glück haben, direkt in Ihrem Spam-Ordner. Allerdings ist dies nur eine mögliche Spielart von Phishing-Angriffen. Dem gegenüber stehen sogenannte Spear-Phishing-Attacken: diese werden von Angreifern professionell auf eine bestimmte Personengruppe zusammengeschnitten und richten sich gegen Personen, über die die Angreifer im Vorfeld Informationen zusammengetragen haben. Dies geschieht vor allem über öffentlich einsehbare Informationen: Telefonbücher, Social-Media-Profile, Job-Profilseiten. Und sobald Angreifern bekannt ist, wo Sie wohnen, welche Art von Auto Sie fahren und wo Sie gerne Urlaub machen, fällt es ihnen einfacher, E-Mails zusammenzubauen, die täuschend echt aussehen und sich für Laien nicht von echten E-Mails unterscheiden lassen. Werden beispielsweise spezielle Abteilungen einer Firma attackiert, lässt sich dies oft einfach mit Informationen aus öffentlichen Quellen anreichern. Oder denken Sie sich etwas dabei, wenn genau die Person, die bei Ihrer Firma am Empfang sitzt, darüber informiert, dass auf dem Firmen-Parkplatz ein Schlüssel gefunden wurde, mit Bild im Anhang, welches genau diesen Parkplatz zeigt? Das Risiko, dass es eine gefälschte E-Mail ist, wird unterschätzt, da es sehr plausibel klingt. Und da der Mensch von sich aus eher konfliktscheu und aus Bequemlichkeit gutgläubig ist, kann sich der Prozentsatz der Personen, die auf eine solche E-Mail reagieren, schnell bei 75 Prozent und mehr bewegen.

> ENGAGIERTE ANGREIFER FINDEN IMMER NEUE ANGRIFFSVEKTOREN UND SICHERHEITSLÜCKEN.

Timo-Sven Johannisson,
Cybersecurity,
Sogeti Deutschland GmbH
www.sogeti.de

Schwachstelle sicher erkennen

Aber zurück zu den E-Mails: es ist natürlich unrealistisch, dass Sie als Privatperson in den Fokus von Kriminellen geraten. Der Aufwand, der betrieben werden muss, ist hoch und die Chance, dass Sie auf diese E-Mail reagieren, sei es Antworten oder Anhänge öffnen oder Links anklicken, dennoch vergleichsweise gering. Realistischer ist es,

DU BIST ANGREIFBAR

dass Sie im Firmenkontext mit Phishing in Berührung kommen. Hier reicht Angreifern, wenn eine einzelne Person auf die E-Mail reagiert. Wird der Versand auf mehrere hundert Personen ausgefahren, steigt somit die Chance für die Angreifer, erfolgreich zu sein. Doch wie kann man sich geeignet verteidigen?

Hauptsächlich besteht eine vernünftige Verteidigung aus zwei Komponenten: Vorsorge und Nachsorge. Implementieren Sie starke Filter und gute Richtlinien, um mögliche Phishing-Attacken frühzeitig abfangen zu können. Ebenso wichtig ist es auch, Notfallpläne auszuarbeiten, was zu tun ist, wenn ein Phishing-Vorfall eintritt. Wer ist zu informieren? Welche Passwörter müssen geändert werden, wie schnell und nach welchen Richtlinien? Und besitzen die Administratoren die Möglichkeit, Accounts und Zugänge schnell zu sperren, um eine Ausweitung des Angriffs im internen Netz eindämmen zu können?

Des Weiteren ist anzumerken, dass die besten Pläne, Vorkehrungen und Maßnahmen nichts nützen, wenn sie nie überprüft oder durchgetestet werden. Aus genau diesem Grund müssen regelmäßig Unterweisungen für Erste-Hilfe-Maßnahmen und Fluchtwege durchgeführt werden. Mit Vorkehrungen gegenüber Angriffen, und darunter fällt auch Phishing, verhält es sich nicht anders: Lassen Sie regelmäßig die Maßnahmen Ihrer Firma gegen unerwünschte E-Mails und Angriffe überprüfen, schulen Sie Ihre Mitarbeiter und beauftragen Sie externe Firmen, die Angriffe für Sie simulieren. Nur so können Sie Angreifern zuvor kommen und verhindern, dass sich Angreifer schnell und ungestört in Ihrem Netzwerken breit machen können.

1. Bewusster Umgang mit Phishing-Attacken

Sie können auch selbst einige Möglichkeiten ergreifen, um es Angreifern schwerer zu machen. Überprüfen Sie, welche Informationen man „von außen" über Sie erhalten kann: Wie sieht Ihre Facebook-Seite aus, wenn Sie nicht eingeloggt sind? Sind andere Social-Media-Profile von Ihnen über Suchmaschinen eventuell einfach zu finden? Muss ihr XING-Profil tatsächlich Informationen über Ihre Hobbies, Ihren Wohnort oder Ihr Auto enthalten?

2. Diskreter Umgang mit Passwörtern

Ein weiterer Punkt ist Passwortsicherheit. Wer die gleichen Passwörter auf unterschiedlichen Webseiten oder Plattformen verwendet, und dann auch noch mit der gleichen Mail-Adresse, riskiert, dass ein Angreifer auf Plattform A auch Ihre Informationen von Plattform B übernehmen kann. Verwenden Sie das gleiche Passwort für Facebook und Spotify, kann ein Angreifer nicht nur Ihre Urlaubsbilder, sondern auch Ihre Musik einsehen. Noch viel einfacher machen Sie es einem Angreifer, wenn Sie sich direkt mit Ihrem Facebook-Account auf Spotify verbinden. Versetzen Sie sich in einen Angreifer hinein und Sie werden verstehen, mit welchen Maßnahmen Sie Angriffe einschränken können und Sie potenziellen Angreifern Steine in den Weg legen. Auch sollten Sie Ihre Passwörter regelmäßig austauschen. Sowohl privat, als auch geschäftlich: Wenn Ihre Firma den Wechsel von Passwörtern nicht vorschreibt oder die Zusammensetzung des Passworts nicht auf Länge, Zeichen-Klassen oder Komplexität überprüft, wird die Hürde für Angreifer, die es gezielt auf diese Firma abgesehen haben, unnötig niedrig gehalten.

3. Sicherung physischer Zugänge für unbefugte Personen

Es ist relevant zu unterscheiden, dass Phishing nicht nur Passwortsicherheit und Social Engineering nicht nur Phishing ist. Wenn Ihre Passwörter stark, Ihre Profile alle geschützt und Ihr Mailsystem gut gefiltert sind, aber ein Angreifer in Ihre Firma laufen und zum Serverraum durchdringen kann, sind sämtliche Maßnahmen überwunden. Es ist somit wichtig, Sicherheit nicht mosaikartig zu betrachten, sondern als Gesamtkonzept: nur wenn alle Angriffsvektoren sowie alle Gegenmaßnahmen erfasst und einzeln sowie als Gesamtkonzept betrachtet und bewertet werden, ist eine realistische Einschätzung

möglich und Hinweise zu weiterführenden Sicherheitsmaßnahmen lieferbar.

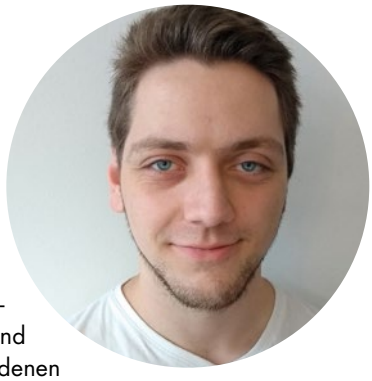
Relevant ist dabei auch eine ungetrübte Sicht „von außen“: Es hilft nichts, wenn der Mitarbeiter, der Firewalls und Passwortrichtlinien erstellt, diese anschließend auch prüft - schließlich bilden die getroffenen Entscheidungen den aktuellen Kenntnisstand des Mitarbeiters ab. Auch könnten größere Umbaumaßnahmen mit Hinweis auf nicht zumutbaren Mehraufwand abgelehnt werden, selbst wenn diese nötig wären. Des Weiteren schließt die Sicht „von außen“ Betriebsblindheit aus. Überprüfungs- und Bewertungsmaßnahmen sollten somit von firmenexternen Fachleuten und Experten regelmäßig durchgeführt werden.

Fazit

Dennoch: Unabhängig davon, welche Maßnahmen gegen Phishing zum Einsatz kommen: Hundertprozentige Sicherheit gibt es nicht und wird es auch nicht geben. Denn engagierte Angreifer können wieder neue Angriffsvektoren finden und diese für die verschiedenen Angriffe verwenden. Auch kommen täglich neue Angriffsmöglichkeiten hinzu, neue Sicherheitslücken werden entdeckt und alte Sicherheitslücken werden bekannter. Passwörter, die vor Jahren als sicher galten, werden heutzutage belächelt, und ähnlich wird es in Zukunft aussehen. Angreifern steht immer mehr Rechenleistung, Dokumentation und Werkzeuge zur Verfügung. Relevant ist, die Hürde so hoch zu legen, dass sich ein Angriff nicht mehr lohnt und nahezu ausgeschlossen werden kann.

Setzen Sie Angreifern alle Steine in den Weg, welche Sie mobilisieren können.

Martin Dessauer, Timo-Sven Johannisson



ÜBERPRÜFUNGS- UND BEWERTUNGSMASSNAHMEN SOLLTEN VON FIRMENEXTERNEN FACHLEUTEN REGELMÄSSIG DURCHGEFÜHRT WERDEN.

Martin Dessauer, Cybersecurity, Sogeti Deutschland GmbH, www.sogeti.de