Fridel Rickenbacher ist Mitbegründer, Partner, Geschäftsführer und Verwaltungsrat der MIT-GROUP, einem Totalunternehmen für «Empowering for the 4th Industrial Revolution» und Informations- und Kommunikationsmanagement. Auf Bundesebene ist er als Experte und Akteur vertreten bei «Digital Dialog Schweiz» + «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS». Er ist in seiner Mission «sh@re to evolve» seit

CyberSecurity und Sicherheit ist eine gemeinsam geteilte Verantwortung

Rund 90% der erfolgreichen und schädigenden Hacker-Attacken bzw. CyberSecurity-Vorfälle basieren auf sogenannten Phishing-Mail-Angriffen oder Social Engineering (Clevere Manipulation der menschlichen Tendenz zum Vertrauen und dem darauf basierten (falschen) Verhalten).

Beitrag von Fridel Rickenbacher

Noch besorgniserregender ist der Fakt, dass die durchschnittliche Erkennungszeit eines solchen gezielten Angriffs mitunter mehrere Monate dauern kann. Die entsprechende, dadurch zusätzlich entstehende Gefahr des weiteren indirekten Schadens oder unerwünschten Nebeneffekten sind je nach Branche oder Ausmass gar existenzbedrohend.

Im Zuge der restriktiver werdenden Regulationen und Compliance-Anforderungen rund um z. B. Datenschutz-Gesetz DSG, Datenschutzgrundverordnung DSGVO / GDPR, Privacy Shield, FINMA können weitere Klagen oder Bussen erwachsen aus solchen erkannten oder unerkannten Gesamt-Sicherheits-Defiziten.

Obwohl die Digitalisierungs- und ICT-Strategie (und integriert die ICT-Sicherheit) – angelehnt an die Firmenstrategie – in der Verantwortung und letztlich auch Haftung der Führungs-Ebene steht, sollten auch die betroffenen Mitarbeiter beteiligt und sensibilisiert/wachsam gemacht werden für den Umgang, Mithilfe und Massnahmen in der dynamischen Bedrohungslage.

Hierzu eignen sich – nebst technischen und organisatorischen Massnahmen – unterstützend auch stufengerecht verständliche Sensibilisierungs-Workshops mit aktuellen Beispielen, Visualisierungen und Erklärungen zur Anatomie von

«Phishing Mail»
Unter dem Begriff Phishing versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Ziel des Betrugs ist es, mit den erhaltenen Daten den entsprechenden Personen oder Firmen zu schaden. Es handelt sich dabei um eine Form des Social Engineering, bei dem die Gutgläubigkeit des Opfers ausgenutzt wird.

«Social Engineering»
Clevere Manipulation der menschlichen Tendenz zum Vertrauen und dem darauf basierten (falschen) Verhalten. Beispiele: Telefonanrufe mit Vortäuschen und Erfragen von Kennwörtern / Bankkonten / sensitive Daten, Phishing Mail.

«Multi-Factor Authentication»
Die Multi-Faktor-Authentifizierung (MFA) ist eine Methode der Computerzugriffskontrolle,

Jahren als Redaktionsmitglied, Experten-Gruppen- und Verbands-Aktivist tätig bei z. B. SwissICT, s-i.ch, isss.ch, isaca.ch, bauen-digital.ch rund um Digitalisierung, Engineering, Clouds, ICT-Architektur, Security, Privacy, Datenschutz, Audit, Compliance, Controlling, Information Ethics, in entsprechenden Gesetzes-Vernehmlassungen und auch in Aus- und Weiterbildung (CAS, eidg. dipl.).

CyberSecurity-Attacken, bewusst wiederkehrende Newsletters oder E-Learning-Modulen mit Tests.

Mittels Weisungen und speziell abgestimmten ICT-Sicherheits-Richtlinien – bei Bedarf als integrierter Bestandteil des Arbeitsvertrages – kann die angestrebt gemeinsam geteilte Verantwortung zur besseren Gesamt-Sicherheit unterstützt werden. Darin sollte auch auf den Schutz des Mitarbeiters durch z. B. klar verständliche Regeln und Abgrenzungen geachtet werden.

Die Mitarbeiter sollten dabei auch technisch unterstützt werden im gemeinsamen Kampf zugunsten des Datenschutzes und Kennwortsicherheit mittels integrierten Lösungen in Bereichen wie z. B. Daten-Verschlüsselung, E-Mail-Verschlüsselung, Multi-Factor Authentication MFA, Information Rights Management IRM / Information Protection oder auch griffigen Kennwort-Richtlinien. Erst dann kann man von Datenschutz sprechen, wenn auch effektiv die eigentliche Datensicherheit maximiert wurde.

Je nach Branche/Funktion und damit allenfalls verbundener, erhöhter Sicherheits-Relevanz können auch bereits bei der Rekrutierung oder im Rahmen der Compliance und Regulation weitergehende Integritäts- oder Sensibilisierungs-Tests gemacht werden zur Erkennung und Beurteilung von firmen- oder projektrelevanten Defiziten oder personenbezogenen Risiken.

Spezielles Augenmerk sollte auf die mobilen/externen Arbeitsplätze, Anwendungen und Geräte im z. B. Aussendienst, Niederlassungen oder Home-Offices gelegt werden mit geeigneten, proaktiven und monitored Services (z. B. vollautomatisierte, regelbasierte Verschlüsselung oder Datenklassifizierung) im Fokus einer integrierten Gesamt-Sicherheits-Lösung.

Zunehmend entstehen auch unterstützende Technologien auf Basis von künstlicher Intelligenz KI / artificial intelligence AI oder machine learning ML – dieses auch nötige «human-machine teaming» (infolge bald erreichten Grenzen von «nur» Technologie) eröffnet völlig neue Komplexitäts-Stufen und Sicherheits-Evolution im CyberSecurity-Bereich – aber leider auch auf Seite der Angreifer.

Die 100% Sicherheit wird es nie geben. Jedoch kann die Technologie + die Prozesse + der Faktor Mensch (human-machine teaming) ein angemessenes Sicherheits-Schutz-Niveau von rund 99% in gemeinsamer Orchestrierung erreichen. Der restliche, nicht erreichbare Anteil ist und bleibt Bestandteil des (Rest-) Risiko-Managements.

bei der ein Benutzer nur dann Zugriff erhält, wenn mehrere Authentifizierungsmechanismen erfolgreich einem bestimmten Authentifizierungsmechanismus präsentiert werden – typischerweise mindestens zwei der folgenden Kategorien: Wissen (etwas, das sie kennen z. B. Kennwort) , Besitz (etwas, das sie haben z. B. Smartphone) und Inhärenz (etwas, das sie sind z. B. E-Mail-Identität).

«CyberSecurity»
CyberSecurity ist eine Sammlung von Richtlinien, Konzepten und Massnahmen, um persönliche oder firmensensitive Daten zu schützen. «CyberSecurity» verbindet technische und organisatorische Aspekte, zum Beispiel Sicherheitssysteme, Prozessdefinitionen, Leitlinien oder Pflichtenhefte. Auch Schulungen zur Sensibilisierung von Mitarbeitern spielen eine wichtige Rolle.