# Expert Notes

*Der regelmässig erscheinende Fachbericht der Neo One zu aktuellen Themen.*


| Nr. 25 | Informieren. | Aufklären. | Sensibilisieren. | neo-one.ch |
|---|---|---|---|---|

Unser Papier besteht zu 100 % aus recycelten Post-Consumer-Fasern und entspricht den höchsten Nachhaltigkeitsstandards. Es ist Co2-neutral, FSC®recycled-zertifiziert, mit dem EU-Umweltzeichen ausgezeichnet und Cradle to Cradle Certified® Bronze zertifiziert.


## *Cyber Security.*
## *Wie sicher ist Ihr Unternehmen?*

*In der Schweiz gehen wöchentlich zwischen 400 und 2000 Meldungen zu Cybervorfällen sowohl von der Bevölkerung wie auch von Unternehmen beim Nationalen Zentrum für Cybersicherheit (NCSC) ein. Diese Zahlen sind nur die Spitze des Eisberges, denn bis anhin war man nicht verpflichtet, entsprechende Vorfälle zu melden. Mögliche Gründe, weshalb Vorfälle nicht gemeldet werden:*

- Es besteht keine Meldepflicht.
- Man will seine Reputation schützen.
- Man weiss nicht, wo man den Vorfall melden kann.
- Man erachtet es nicht als wichtig.
- Kein Vertrauen in die Meldestelle.

Die Meldepflicht wird sich mit der Einführung des neuen revidierten Datenschutzgesetzes revDSG und ab 2024 bzw. 2025 auch gemäss ISG teilweise ändern und für gewisse Thematiken im Bereich Datenschutzverletzung zwingend werden.
Häufig handelt es sich bei den Cyberangriffen um Betrugs- und Phishing-Vorfälle (mehr zu Phishing weiter unten in diesen Expert Notes). Meistens geht es den Hackern um Zugriffe auf sensible Informationen, Manipulation oder Zerstörung von wichtigen Daten, Erpressung oder Störung der Geschäftsprozesse. Der technische Fortschritt kommt dabei auch den Cyberkriminellen zugute: Mit neuartigen Angriffen basierend auf KI (künstlicher Intelligenz), digitalen Supply-Chain-Attacken u. v. m. muss künftig vermehrt gerechnet werden.
Das Thema Cyber Security ist wichtiger denn je – für KMU, für grössere Unternehmen und öffentliche Dienste, aber auch für jeden einzelnen von uns. In Unternehmen kommt es mehr denn je auch auf die Wachsamkeit der Mitarbeitenden und eine starke Sicherheitskultur an – mehr dazu weiter unten in diesen Expert Notes (Mitarbeitenden-Vulnerability).

*«Die grösste Gefahr ist, sich in falscher Sicherheit zu wiegen. Sowohl in der Wirtschaft als auch in der Gesellschaft setzt sich das fatale Gefühl fest, dass es einen schon nicht treffen wird.»*

***Michel Hipp, CIO***

## ***Cyber Security Report.***
## *Die Wahrheit über unsere Daten.*

*Ein Blick in den Cyber Security Report zeigt die Dringlichkeit nach umfassenden und nachhaltigen Lösungen für Unternehmen und öffentliche Dienste.*

Der Schwarz Cyber Security Report zum laufenden Jahr zeigt deutlich: Cyber Sicherheit und Cyber Defense sollte jedes Unternehmen zur obersten Priorität erklären. Denn private und staatliche Akteure professionalisieren sich zusehends im Bereich Cyberkriminalität und Cyberattacken.

(Quelle: Die Cyber Security Conference / Cyber Security Report by Schwarz. https://cyberconference.schwarz/)

**Fakten zur Daten(un)sicherheit**
Cyberrisiken sind laut dem Allianz Risk Barometer 2022 sowie den Erhebungen des Bundes zur grössten Gefahr für Unternehmen geworden – vor Betriebsunterbrechungen, Naturkatastrophen und dem erneuten Ausbruch einer Pandemie.

**Cyberangriff**
Alle mindestens 39 Sekunden erfolgt irgendwo auf der Welt ein Cyberangriff.

**Ransomware-Angriffe**
71 % der Organisationen weltweit wurden 2022 Opfer von Ransomware-Angriffen.

39 71

**Jährliche Kosten**
Die jährlichen globalen Kosten der Cyberkriminalität werden bis 2026 auf jährlich 20 Billionen Dollar geschätzt.

20

**Drei Schritte**
In fast 75 % der Fälle brauchen Hacker weniger als drei Schritte, um an sensible Systeme und Daten eines Unternehmens oder einer Organisation des öffentlichen Sektors zu gelangen.

3/4 75

**Schwachstellen**
¾ der identifizierten Schwachstellen erlaubten es, zu den wichtigsten Systemen der Unternehmensnetzwerke zu gelangen oder wichtige Daten aus der Cloud abzugreifen.

*«Diejenigen, die es getroffen hat, warnen eindringlich, alles zu tun, damit man das nicht erleben muss.»*

***Patrick Stalder, CIO***

Private Unternehmen sowie auch Organisationen im öffentlichen Sektor weisen unfassbar viele Sicherheitslücken in ihren Systemen auf, die sozusagen auf dem Silbertablett serviert werden und es Angreifern leicht machen, Daten abzugreifen. Solche Sicherheitslücken entstehen zum Beispiel durch

- Fehlkonfigurationen
- Ungenügend konfigurierte Systeme
- Fehlende oder nicht ausreichende Aktualisierungen
- Schwache Passwörter und unsichere Authentisierungen
- Falsch verwaltete Benutzerkonten
- Unzureichende Zugriffskontrollen
- Veraltete Verschlüsselungsmethoden
- Keine ganzheitliche Sicherheitsstrategie
- Social Engineering
- Ungenügend geschulte Mitarbeitende
- Zero-Day-Exploits

## *Die 8 grössten Angrifftrends 2023.*

*1*

**Künstliche Intelligenz (KI) und Machine Learning (ML)**

- KI bezieht sich auf die Simulation menschlicher Intelligenz in Computern. ML: Eine Art von KI. Beim Machine Learning lernen Computer aus Daten und versuchen, Muster zu erkennen.

*2*

**Ransomware-Angriffe & Ransomware as-a-Service**

- Ransomeware ist eine Form von Schadsoftware (Malware), die entwickelt wurde, um Dateien oder Systeme zu verschlüsseln oder zu sperren und dann von den Opfern ein Lösegeld (Ransom) zu erpressen.

*3*

**Der Dauerbrenner Phishing**

- Phishing ist eine Form von Cyberangriff, bei der Angreifer sich als vertrauenswürdige Quellen ausgeben, um Informationen von Opfern zu stehlen. Der Begriff «Phishing» leitet sich von «Fischen» ab, da die Angreifer nach sensiblen Informationen «angeln».

*4*

**Digitale Supply Chain Angriffe**

- Digitale Supply Chain-Angriffe beziehen sich auf Cyberangriffe, bei denen Angreifer gezielt die Lieferkette eines Unternehmens angreifen, um Schwachstellen auszunutzen, Daten zu stehlen, die Verfügbarkeit von Produkten oder Dienstleistungen zu beeinträchtigen.

*5*

**IoT Bedrohungen und Angriffe auf vernetzte Geräte**

- IoT bedeutet Internet of things, zu Deutsch Internet der Dinge. Die Vernetzung von physischen Geräten, Sensoren und Objekten mit dem Internet, um Daten zu sammeln, zu übertragen und zu analysieren, wird ausgenutzt, um Cyber-Angriffe zu vollziehen.

*6*

**Staatlich gestützte Angriffe, geopolitische Konflikte, globale Spannungen**

- Staatlich gestützte Angriffe sind Cyberangriffe, bei denen eine nationale Regierung oder eine staatliche Einrichtung direkt oder indirekt beteiligt ist oder diese unterstützt.

*7*

**Social Engineering in Kombination mit Multi-Channel Phishing**

- Social Engineering / Multi-Channel Phishing: Eine ausgefeilte Taktik, die von Cyberkriminellen verwendet wird, um Opfer zu täuschen und sensible Informationen zu stehlen oder schädliche Handlungen auszuführen. Diese Methode kombiniert verschiedene Kommunikationskanäle und soziale Manipulation, um die Chancen eines erfolgreichen Angriffs zu erhöhen.

*8*

**Angriffe auf ungenügende Authentisierungen**

- Angriffe auf ungenügende Authentisierungen sind erfolgreich, weil Sie auf ein System oder eine Anwendung abzielen, die nicht ausreichend geschützt ist (Authentifizierung und Zugriffskontrolle).

## ***Die Schweiz.***
## *Attraktives Ziel für Cyperangriffe.*

*Die Schweiz als eine sehr starke Wirtschaftsnation ist ein attraktives Ziel für Cyberkriminelle, die auf finanzielle Gewinne, Diebstahl von geistigem Eigentum und politische Einflussnahme abzielen.*

**Signifikante Zunahme der Cyberangriffe:**
Die Zahl der Angriffe hat in den letzten Jahren in der Schweiz stark zugenommen, allein im Jahr 2022 um 61 % gegenüber dem Vorjahr. Die Angriffe reichen von Phishing-Attacken und Ransomware-Angriffen bis hin zu gezielten Angriffen auf Unternehmen und staatliche Institutionen.

**Bedrohung kritischer Infrastrukturen:**
Energieversorgung, Gesundheitswesen, Finanzsektor – diese Infrastrukturen sind besonders anfällig für Cyberangriffe, da Störungen erhebliche Auswirkungen auf die nationale Sicherheit und die Wirtschaft haben.

**Fachkräftemangel:**
Die Nachfrage nach qualifizierten Cyber Security-Experten übersteigt das Angebot, was die Fähigkeit zur Erkennung und Abwehr von Angriffen einschränkt.

**Neues Datenschutzgesetz:**
Das neue Datenschutzgesetzt hat erhebliche Auswirkungen auf die Cybersicherheit. Es stärkt die Rechte zur Kontrolle der persönlichen Daten und verpflichtet Unternehmen und Organisationen zu strengeren Datenschutz- und Sicherheitsstandards.

**Internationale Zusammenarbeit:**
Die Schweiz arbeitet eng mit anderen Ländern und internationalen Organisationen zusammen, um sich gegen grenzüberschreitende Cyberbedrohungen zu verteidigen. Diese Zusammenarbeit ist entscheidend, da viele Angriffe von ausländischen Akteuren ausgehen.

Insgesamt erfordert die aktuelle Lage in der Schweiz eine noch stärkere Sensibilisierung für die Themen Sicherheit, Investitionen in Technologien und Fachkräfte sowie die Anpassung an die neuen Datenschutzbestimmungen.
Verschliesst man sich diesen Massnahmen, gefährdet man nicht nur sein eigenes Unternehmen, sondern auch die Unternehmen, mit denen man Geschäfte macht. So können Hacker bei einem Cyberangriff Schwachstellen nutzen, um sich Zugang zu einem Lieferanten, Kunden oder Mitarbeitenden zu beschaffen. Nicht zuletzt deshalb ist es richtig, dass die EU und jetzt auch die Schweiz mit dem neuen Datenschutzgesetz für alle strenge Auflagen schaffen, die damit auch zur besseren Cyber-Resilienz beitragen.

## ***Die Folgen der Pandemie.***
## *Der Preis des digitalen Fortschritts.*

*Gemäss dem Cyber Security-Anbieter Check Point und diversen Umfragen und Studien verzeichnen KMU-Anbieter branchenunabhängig sowie die generelle Finanz- und Kommunikationsbranche in der Schweiz die stärkste Zunahme von Cyberangriffen.*

Für die Zunahme können drei Trends ausgemacht werden:

- schnelle Entwicklung des Ransomware-Ökosystems mit kleineren, agileren kriminellen Gruppen
- erweiterung der Phishing-Exploits auf Kollaborationstools wie Slack, Teams, OneDrive und Google Drive – allesamt ergiebige Quellen für sensible Daten
- die grossen Sicherheitslücken bei akademischen Betrieben und KMU, die als Reaktion auf die Pandemie eine (zu) rasche Digitalisierung vornehmen mussten

| | |
|---|---|
| **Remote-Arbeit** | Für die Umstellung auf Remote-Arbeit, bzw. Homeoffice, wurde oft keine ausreichende Sicherheitsinfrastruktur bereitgestellt. Die Angriffe auf Remote-Verbindungen, VPN sowie auf Tools wie Slack, Teams oder Google Drive nehmen zu. |
| **Verstärkte Online-Aktivitäten** | Während der Pandemie haben viele Menschen viel mehr Zeit online verbracht. Für die Arbeit, für die Schule oder in der Freizeit. Dies hat Cyberkriminellen mehr Gelegenheit gegeben, um Phishing-Angriffe, Ransomware-Angriffe und andere Arten von Cyberangriffen durchzuführen. |
| **Überlastung der Sicherheitsinfrastruktur** | Die abrupte Verschiebung vieler Aktivitäten in den Online-Modus hat die Sicherheitsinfrastrukturen vieler Organisationen überlastet, Schwachstellen wurden übersehen oder nicht rechtzeitig behoben. |
| **Mangelndes Sicherheitsbewusstsein** | Während der Pandemie waren viele Menschen mit der Anpassung an neue Arbeits- und Lebensbedingungen beschäftigt. Dies führte zu einem Mangel an Aufmerksamkeit für die Cybersicherheit, was Angreifern das Eindringen in Systeme erleichterte. |
| **Mangelnde Fachkenntnisse der ICT Branche** | Viele ICT Anbieter und ICT Dienstleister verzeichnen leider ein mangelhaftes Know-how und sind nicht up to date, bzw. auf einem Stand von vor zehn Jahren, in den Bereichen Installationen, Konfigurationen, Beratungen, Wartungskonzept und Supportleistungen. Die wichtige Thematik ICT Security wird nicht in den Umsetzungen adressiert. |

Neben dem raschen digitalen Fortschritt und der Weiterentwicklung von KI sind es also auch die Spätfolgen der Pandemie, die für verstärkte Cyberkriminalität verantwortlich sind. Denn: Während der Pandemie haben viele Organisationen und Unternehmen ihre Aktivitäten verstärkt digitalisiert.

## ***Wo steht mein Betrieb?***
*Klarheit ist der erste Schritt.*

Der Schaden durch Hackerangriffe ist immens. Dabei liessen sich solche kriminellen Attacken abwehren – mit den richtigen Sicherheitsmassnahmen. Natürlich kommt aktuell noch die Einführung des neuen Datenschutzgesetzes hinzu, das zusätzliche Anpassungen, Investitionen und Dokumentationen erfordert. Aber andererseits bietet sich damit auch eine gute Gelegenheit, die Cybersicherheit des eigenen Unternehmens unter die Lupe zu nehmen, eine ganzheitliche Betrachtungsweise einzunehmen und die detailgetreue Bestandesaufnahme des IST-Zustandes zu beleuchten.

*«Security by Design, Cybersicherheit und Datenschutz müssen ganzheitlich im Unternehmen adressiert werden.»*

***Manuel Caprioli***
***Senior ICT System Engineer & Senior ICT Consultant***

Für Ihr Unternehmen oder Ihre Organisation heisst das:

### 1. SCHRITT: DIE DETAILLIERTE ANALYSE ALS SOLIDE BASIS

- Detaillierte ICT Situationsanalyse zur Sicherstellung aller Basisinformationen und Grundlagen wie der Betrieb Stand heute operiert, funktioniert und aufgestellt ist
- Detaillierte ICT Funktionsüberprüfungen zur Sicherstellung von IST/SOLL-Zuständen
- Detaillierte ICT Organisationsprüfung der ICT Aufbau- und Ablauforganisation
- Detaillierte Sicherheitsüberprüfungen der ICT Security und Cyber-Defense
- Überprüfung Datenschutz, Protokollierungen, Dokumentationen, Prozesse, Reglemente, Notfallkonzepte
- Detaillierte Bedürfnisabklärung bei dezidierten Abteilungen und Mitarbeitenden
- Detaillierte Überprüfung von Abläufen und Tätigkeiten wie Support, Wartung, Monitoring
- Überprüfung von aktuellen Konzepten, Strategien, Vorgehensweisen und Abläufen

### 2. SCHRITT: BERICHT, RISIKOBEWERTUNG, HANDLUNGSFELDER-ÜBERSICHT, MANAGEMENTCOCKPIT

- Detaillierte Berichterstellung mit einer ganzheitlichen Ansicht der aktuellen Lage
- Exakt gesonderte Aufstellung von Risikobewertungen
- Exakte Aufstellung von besonders schützenswerten Assets im Unternehmen
- Realistische und umsetzbare Darstellung aller Handlungsfelder inkl. Bewertung der Kritikalität und Dringlichkeit
- Kosten/Budget für notwendige Umsetzungen der Handlungsfelder und benötigten Interventionen
- Daraus resultierendes Managementcockpit für die Entscheidungsträger und verantwortlichen Gremien

### 3. SCHRITT: PRÄSENTATION, AUFKLÄRUNG, SENSIBILISIERUNG

- Präsentation der Sachlage vor den Entscheidungsgremien
- Einfach verständliche Erläuterungen zur aktuellen Lage
- Verständnisförderung der komplexen Thematik
- Aufklären und Kommunikation der wichtigen Kausalitäten

*«Komplexität und Interkonnektivität sind ein Risiko, dem mehr Beachtung geschenkt werden sollte. Die rasant und stetig zunehmende Komplexität im Bereich ICT und die fortlaufende Vernetzung von Geräten und Systemen, sei es im Business Umfeld oder in der Gesellschaft, führen vermehrt dazu, dass Sicherheitslücken übersehen werden oder zu wenig konzeptionelle Anstrengungen unternommen werden, um diese zu verhindern oder zubeheben.»*

***Jan Keller, Senior ICT System Engineer & Senior ICT Consultant***

## ***Mitarbeitenden-Vulnerability.***

*Sichere Mitarbeitende, sicherer Betrieb.*

*Die Untersuchung von Mitarbeitenden-Vulnerability (Verletzlichkeit von Mitarbeitenden) ist ein wichtiger Aspekt im Bereich der Unternehmenssicherheit.*

Bei der Prüfung geht es darum, potenzielle Schwachstellen und Risiken zu identifizieren, denen Mitarbeitende ausgesetzt sein könnten, und entsprechende Massnahmen zu ergreifen, um diese zu minimieren oder zu beseitigen.

In folgenden Bereichen lohnt es sich, die Mitarbeitenden-Vulnerability zu prüfen:

### PHISHING UND SOCIAL ENGINEERING

Überprüfung der Anfälligkeit der Mitarbeitenden für Phishing-Angriffe, betrügerische E-Mails oder Anrufe, bei denen versucht wird, vertrauliche Informationen zu erhalten.

### CYBER SECURITY-SCHULUNGEN

Beurteilung des Kenntnisstands der Mitarbeitenden in Bezug auf Cybersicherheitspraktiken und -richtlinien.

### GERÄTESICHERHEIT

Untersuchung der Sicherheitsvorkehrungen auf den von Mitarbeitenden verwendeten Geräten (Computer, Smartphones usw.) und deren Aktualisierungsstatus.

### PHYSISCHE SICHERHEIT

Prüfung der Sicherheitsvorkehrungen am Arbeitsplatz, einschliesslich Zugangsbeschränkungen und Massnahmen zur Verhinderung unbefugten Zutritts.

### DATENSCHUTZ

Überprüfung der Handhabung sensibler Daten durch Mitarbeitende, um sicherzustellen, dass Datenschutzbestimmungen und -richtlinien eingehalten werden.

### EXTERNE GERÄTE UND MEDIEN

Prüfung der Sicherheitsmassnahmen beim Umgang mit externen Speichermedien (USB-Laufwerke, externe Festplatten) und anderen Geräten, die an Unternehmenssysteme angeschlossen werden.

### HOMEOFFICE-SICHERHEIT

Analyse der Sicherheitsmassnahmen für Mitarbeitende, die remote arbeiten, um sicherzustellen, dass ihre Heimarbeitsumgebung geschützt ist.

### PASSWORTSICHERHEIT

Analyse der Passwortrichtlinien und -praktiken der Mitarbeitenden, um zu überprüfen, ob starke Passwörter verwendet werden und wie gut diese geschützt sind.

### NOTFALLMASSNAHMEN

Überprüfung der Kenntnisse der Mitarbeitenden über Notfallpläne und ihre Fähigkeit, angemessen auf Sicherheitsvorfälle zu reagieren.

Die genauen Aspekte können je nach Unternehmenskontext und -bedürfnissen variieren. Es ist wichtig, eine umfassende Bewertung durchzuführen, um die Sicherheit der Mitarbeitenden und des Unternehmens zu gewährleisten.

*«IT-Sicherheit geht jeden an – alle im Unternehmen sind Teil davon. Nur mit ganzheitlichen Ansätzen ist ein Unternehmen besser geschützt.»*

***Daniel Puschl, Senior ICT System Engineer & Senior ICT Consultant***

### REMOTE-ZUGRIFF UND VPN-NUTZUNG

Bewertung der Sicherheitsprotokolle für den Zugriff auf Unternehmensressourcen über VPN oder andere Remote-Verbindungen.

### SICHERHEITSBEWUSSTSEIN

Einschätzung des allgemeinen Sicherheitsbewusstseins der Mitarbeitenden und ihrer Bereitschaft, Sicherheitsrichtlinien und -verfahren zu befolgen.

### KOMMUNIKATION

Analyse der internen Kommunikationsrichtlinien und -praktiken, um sicherzustellen, dass Mitarbeitende angemessen über Sicherheitsbedenken informiert werden.

### EINHALTUNG VON RICHTLINIEN

Überprüfung, ob Mitarbeitende Unternehmensrichtlinien und -verfahren befolgen, insbesondere in Bezug auf Sicherheit.

### BERICHTERSTATTUNG VON SICHERHEITSVORFÄLLEN

Untersuchung der Wirksamkeit der internen Meldeverfahren für Sicherheitsvorfälle und -verletzungen.

### SICHERHEITSSOFTWARE UND -TOOLS

Bewertung der Nutzung von Antivirus-Software, Firewall, Verschlüsselungstools und anderen Sicherheitsanwendungen.

## ***Nice to know.*** *Was ist Phishing?*

Wissen ist Macht – je mehr man weiss, je sicherer ist man unterwegs. Deshalb ist es gut zu wissen, was hinter den viel zitierten Schlagwörtern im Zusammenhang mit Cyberangriffen steckt. Zum Beispiel: Was bedeutet eigentlich «Phishing»? Unter dem Begriff Phishing versteht man die unrechtmässige Beschaffung von persönlichen Daten über gefälschte Websites, E-Mails oder Kurznachrichten. Die Betrüger erstellen dazu beispielsweise eine gefälschte, aber identisch aufgestellte Webseite einer Bank, eines E-Mail-Providers oder einer Shopping-Seite. Beim Phishing wird der User dazu verleitet, Links anzuklicken und so womöglich auf eine gefälschte Website zu kommen. Nicht nur Privatpersonen, auch Unternehmen werden immer öfter Opfer von Phishing-Attacken. Auf diese Weise wollen die Betrüger an persönliche Daten gelangen. Die Fälschungen werden immer besser, so dass leider viele auf die Betrugsmasche reinfallen.

Die registrierten Phishing-Fälle in der Schweiz haben 2022 um 84,8 % gegenüber dem Vorjahr zugenommen. Die polizeiliche Kriminalstatistik (PKS) führt dazu 2236 Fälle im letzten Jahr auf.

## ***Die Schritt-für-Schritt-Anleitung.***
## *Für mehr Sicherheit in Ihrem Unternehmen.*

*Die Trainings-Phishing-Kampagne für Mitarbeitende ist eine effektive Methode, um das Bewusstsein für Cybersicherheit zu schärfen und die Mitarbeitenden gegen Phishing-Angriffe zu sensibilisieren.*

### ***Schritt 1***
*Zielsetzung definieren*

Bestimmen Sie das Hauptziel der Kampagne.

A) Sie möchten das allgemeine Bewusstsein für Phishing steigern und eines oder mehrere Training-Phishing-Mails an alle im Unternehmen versenden.

B) Sie möchten spezifische Sachverhalte auf Ihre Unternehmensabläufe gerichtet testen und adressieren, indem Sie gezielte Versände an Abteilungen unterschiedlich lancieren.

### ***Schritt 2***
*Ressourcen und Zuständigkeiten festlegen*

Definieren Sie den Verantwortlichen für diese Kampagne und halten Sie den Personenkreis der Involvierten äussert klein.

### ***Schritt 3***
*Phishing-Szenario entwickeln*

Erstellen Sie realistische Phishing-Mails oder Nachrichten, die

A) den gängigen Phishing-Angriffen ähneln, die in Ihrer Branche oder in Ihrem Unternehmen vorkommen.

B) aktuelle Themen, Bereiche, Gegebenheiten, Sachverhalte in Ihrem Unternehmen wiedergeben.

### ***Schritt 4***
*Zielgruppen auswählen*

Basierend auf den Punkten oben gilt es nun, die genauen Zielgruppen zu definieren.
Teilen Sie Ihre Mitarbeitenden in verschiedene Gruppen auf und planen Sie, die Phishing-Mails an diese Gruppen zu senden. Stellen Sie sicher, dass Sie die Zustimmung der Geschäftsleitung und/oder des Verwaltungsrats haben.

### ***Schritt 5***
*Versand*

Versenden Sie die vorbereiteten Phishing-Mails an die ausgewählten Gruppen bewusst an unterschiedlichen Tagen.

### ***Schritt 6***
*Verfolgen, überwachen, auswerten*

Verfolgen Sie, wie die Mitarbeitenden auf die Phishing-Mails reagieren. Erfassen Sie Daten darüber, wer auf die Links geklickt oder sensible Informationen preisgegeben hat. Werten Sie die Ergebnisse aus.

### ***Schritt 7***
*Abschluss der Kampagne*

Leiten Sie Information über die gesamte Kampagne und die Resultate und Erkenntnisse an die Geschäftsleitung.

### ***Schritt 8***
*Information, Schulung und Sensibilisierung*

Präsentieren Sie das anonymisierte Resultat in einer Schulung, erklären Sie, was verbessert werden kann, geben Sie Tipps und erläutern Sie die Gefahren.

### ***Schritt 9***
*Information, Schulung und Sensibilisierung*

Wiederkehrende Kampagnen bringen den Erfolg. Einmal jährlich sollten Sie eine lancieren.