ISO 27001:
Zertifizieren Sie Ihr Unternehmen in 14 Schritten schnell und einfach!

CYBERXPERTS

Inhaltsverzeichnis

ISO 27001: Warum KEIN Unternehmen langfristig mehr auf die Zertifizierung verzichten kann

Liebe Leserin, lieber Leser,

Informationssicherheit ist gerade in der heutigen Zeit unverzichtbar. Sie muss als Bestandteil der Unternehmensführung darauf ausgerichtet sein, die Geschäftsziele optimal zu unterstützen. Gerade angesichts der aktuellen Cyberbedrohungen ist ein gut strukturiertes Informationssicherheitsmanagementsystem (ISMS) nach international anerkannten Standards die optimale Grundlage zur effizienten und effektiven Umsetzung einer ganzheitlichen Sicherheitsstrategie.

Die ISO 27001:2013 ist der internationale Standard für Informationssicherheitsmanagementsysteme. Unternehmen können ihr ISMS nach dieser Norm zertifizieren lassen. Für Sie als Informationssicherheitsbeauftragter (ISB) oder Geschäftsführer bietet eine solche Zertifizierung die Chance, die Informationssicherheit im Unternehmen nachhaltig und ganzheitlich voranzubringen. Angesichts der sehr hohen Schäden durch Cybercrime im Jahr 2022 ist es höchste Zeit zu handeln. Investieren Sie als Geschäftsführer oder ISB in Ihr ISMS und schützen Sie so Ihr Unternehmen vor existenzbedrohenden Schäden. Sie werden sehen, dass ein ISMS keine Raketentechnik ist. Im Gegenteil – es geht gerade nicht um Technik. Es geht in erster Linie um die Etablierung sachgerechter und wirksamer Prozesse, die unter Risikogesichtspunkten Ihre Unternehmenswerte schützen.

Andreas Hessel,CISO, BCM-Beauftragter, IS-Risikomanager

Naomi Meier, Online-Trainerin CyberXperts

„Die Lage ist ernst …“ – Warum ein ISMS nicht nur in den KRITIS sinnvoll ist

Wie ein unzureichendes ISMS die aktuelle Cyber-Sicherheitslage bedroht

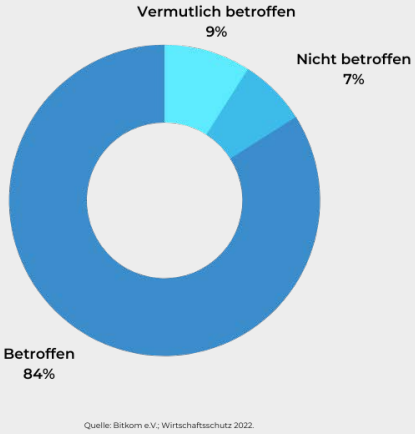
Die ISO 27001:2013 spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagements unter Berücksichtigung der Informationssicherheitsrisiken innerhalb des gesamten Unternehmens.

Ein ISMS nach ISO 27001:2013 ist die Basis dafür, dass die Vertraulichkeit, Verfügbarkeit und Integrität von Unternehmenswerten (Informationen) effektiv geschützt werden können. Denn nur durch standardisierte Sicherheitsmaßnahmen (Soll) kann die Effektivität eines ISMS (Ist) überprüft werden.

Die Risiken eines unzureichenden ISMS zeigen aktuelle Studien. Danach waren 84 Prozent der Unternehmen in Deutschland im Jahr 2021 von einem Cyberangriff betroffen, weitere 9 Prozent gehen davon aus.[1] Zugleich gehen die Angreifer immer professioneller vor. Erstmals liegen das organisierte Verbrechen und Banden an der Spitze der Rangliste der Täterkreise.

1 Bitkom e. V., Wirtschaftsschutz 2022, https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf, abgerufen am 18.11.22.

84 Prozent der Unternehmen in Deutschland waren 2021 von einem Cyberangriff betroffen

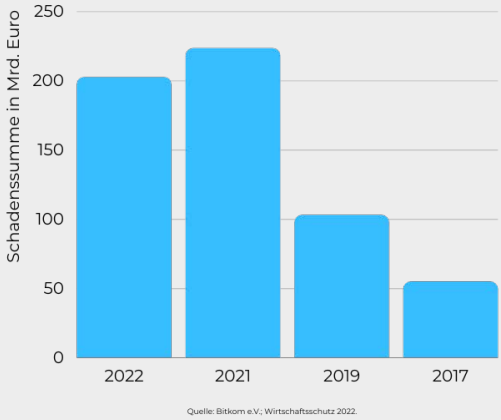


Quelle: Bitkom e. V. Wirtschaftsschutz 2022

Der deutschen Wirtschaft entstand im Jahr 2022 ein Schaden von rund 203 Milliarden Euro durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage. Damit liegt der Schaden etwas niedriger als im Rekordjahr 2021 mit 223 Milliarden Euro. In den Jahren 2018/2019 waren es erst 103 Milliarden Euro.[2]

2 Bitkom e. V., Wirtschaftsschutz 2022, https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf, abgerufen am 18.11.22.

Fast 203 Milliarden Euro Schaden pro Jahr durch Diebstahl, Industriespionage oder Sabotage



Quelle: Bitkom e. V. Wirtschaftsschutz 2022

Wichtige Definitionen:

IT-Sicherheit und Informationssicherheit werden oft synonym verwendet. IT-Sicherheit ist jedoch nur ein Teilaspekt der Informationssicherheit. Während die IT-Sicherheit sich auf den Schutz von technischen Systemen bezieht, geht es in der Informationssicherheit allgemein um den Schutz von Informationen. Diese können auch in nicht-technischen Systemen vorliegen, z. B. auf Papier. Die Schutzziele der Informationssicherheit bestehen darin, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen.

Cybersicherheit ist die Praxis des Schutzes kritischer Systeme und vertraulicher Informationen vor digitalen Angriffen. Cybersicherheitsmaßnahmen sind darauf ausgerichtet, Bedrohungen für vernetzte Systeme und Anwendungen entgegenzuwirken, unabhängig davon, ob diese Bedrohungen von innerhalb oder außerhalb eines Unternehmens ausgehen.

Cyber-Resilienz ist die Fähigkeit eines Unternehmens oder einer Organisation, ihre Geschäftsprozesse trotz widriger Cyber-Umstände aufrechtzuerhalten. Das können Cyberangriffe sein, aber auch unbeabsichtigte Hindernisse wie ein fehlgeschlagenes Software-Update oder menschliches Versagen. Cyber-Resilienz ist ein umfassendes Konzept, das über die IT-Sicherheit hinausgeht.

18.712 € Kosten pro Jahr durch Cyberangriffe: Warum sich ein ISMS für Sie IMMER lohnt[3]

Als Sicherheitsbeauftragter werden Sie bei Ihrem Vorhaben immer auf Gegenargumente wie „zu teuer", zu „komplex und aufwendig" und „kein Nutzen" stoßen. Sie sollten daher mit Ihrer Geschäftsleitung und der IT-Abteilung sprechen und auf die folgenden Synergieeffekte bei einer Zertifizierung hinweisen:

- Verbesserte Wahrnehmung der IT im Unternehmen durch Offenlegung der Abhängigkeit von Geschäftsprozessen (Ohne IT geht gar nichts!)
- Verbesserte Dokumentation und Transparenz in der IT (Strukturanalyse, Schutzbedarf)
- Steigerung der Effektivität durch optimierte Prozesse in der IT (Störungsmanagement, Change Management usw.)
- Regelmäßige Schulungsmaßnahmen (Minimierung von Fehlern und Supportaufkommen)
- Ressourcen- und Kostenoptimierung (Beschränkung auf das Wesentliche)
- Bessere Verfügbarkeiten durch Identifizierung von Schwachstellen

Mein Tipp: Weisen Sie Ihre Geschäftsleitung und IT-Abteilung darauf hin, dass eine Zertifizierung nach ISO 27001:2013 eine klassische Win-win-Situation bietet. Die Zertifizierung etabliert zwar in erster Linie ein ISMS, aber von den Synergieeffekten profitiert am stärksten die IT-Abteilung.

3 Hiscox, Cyber Readiness Report 2022, https://www.hiscox.de/cyber-readiness-report-2022/, abgerufen am 13.12.2022.

10-Punkte-Check: So prüfen Sie Ihr aktuelles Sicherheitslevel

Die konkrete Einführung eines ISMS erfordert Erfahrung, basiert allerdings zwingend auf der Entscheidung und Verpflichtung der obersten Leitungsebene gegenüber dem Thema. Ein klarer Managementauftrag und eine an die Geschäftsstrategie angepasste Sicherheitsstrategie sind zusammen mit kompetentem Personal und den letztlich immer erforderlichen Ressourcen die Grundvoraussetzungen, um mit einem ISMS die Erreichung der Geschäftsziele optimal unterstützen zu können.

Die Zertifizierung muss durch einen zertifizierten Auditor durchgeführt und von einer entsprechenden Prüfungsstelle abgenommen werden. Hierbei werden folgende Schritte durchlaufen:

1. Definition des Geltungsbereiches des ISMS (das ganze Unternehmen, nur kritische IT-Infrastrukturen, kritische Geschäftsbereiche usw.)
2. Durchführung eines Voraudits (Erhebung der IST-Situation)
3. Durchführung des Audits Stufe 1 durch einen zertifizierten Auditor (Sichtung der Dokumente)
4. Durchführung des Audits Stufe 2 durch einen zertifizierten Auditor (Inspektion vor Ort)
5. Ausstellung des Prüfberichts und des Zertifikats, das eine Gültigkeit von drei Jahren hat und jährlich überwacht wird

Eine Zertifizierung kann nur dann erfolgreich sein, wenn die Unternehmensleitung diesen Prozess unterstützt. Auch die IT-Abteilung und alle Fachbereiche sind in eine Zertifizierung eng eingebunden. Die IT-Abteilung muss alle erforderlichen Richtlinien und Dokumentationen erstellen und in der Regel neue Prozesse etablieren. Das ist immer mit einem erheblichen Aufwand und hohen Kosten verbunden.

Prüfen Sie diese 10 Punkte vor einer Zertifizierung

Sie können als Geschäftsführer oder ISB gemeinsam mit Ihrer IT-Abteilung bereits vor einer Zertifizierung prüfen, wo Sie mit Ihrem ISMS stehen. Nutzen Sie dazu die folgende Checkliste.

Checkliste: ISMS nach ISO 27001:2013 – was ist bereits etabliert?		
Anforderung	**Ja**	**Nein**
Existiert eine Informationssicherheitsleitlinie und ist diese von der Unternehmensleitung verabschiedet?	☐	☐
Gibt es ein von der Unternehmensleitung verabschiedetes Budget für Maßnahmen in der Informationssicherheit?	☐	☐
Ist ein Informationssicherheitsbeauftragter (ISB) (für Informationssicherheit verantwortliche Stelle/Person/Mitarbeiter) bestellt und berichtet dieser direkt an die Unternehmensleitung?	☐	☐
Wurde von der IT-Abteilung eine Strukturanalyse (Erhebung aller IT-Ressourcen wie Gebäude, Serverräume, IT-Systeme, Anwendungen, Netze usw.) durchgeführt?	☐	☐
Wurde von der IT-Abteilung eine Schutzbedarfsanalyse durchgeführt und wurde für alle Daten und Anwendungen von den Dateneigentümern (Fachbereichen) ein Schutzbedarf (Vertraulichkeit, Verfügbarkeit, Integrität) festgelegt?	☐	☐
Wurden Schwachstellen identifiziert und die daraus resultierenden Risiken mit geeigneten Maßnahmen minimiert?	☐	☐
Gibt es Regelungen zur Zutrittskontrolle im Unternehmen und existieren Regelungen für besonders kritische Räumlichkeiten (Serverräume etc.)?	☐	☐
Ist der Umgang mit Sicherheitsvorfällen/Datenpannen (Meldewege, Notfallmaßnahmen usw.) geregelt?	☐	☐
Werden die Mitarbeiter regelmäßig zu IT-Sicherheitsthemen und zu den internen Richtlinien geschult?	☐	☐
Existieren Notfallpläne für den Ausfall von IT-Systemen, Gebäuden, Personal und Dienstleistern?	☐	☐

In der Regel wird Ihre IT-Abteilung zu vielen Anforderungen der Checkliste Regelwerke haben oder konkrete Maßnahmen umsetzen, gehören sie doch zum normalen IT-Betrieb. Sie müssen also Ihre IT-Abteilung davon überzeugen, dass die Zertifizierung keine Raketentechnik ist. Es gilt in erster Linie, das „Gelebte“ zu optimieren, geregelte Prozesse zu etablieren und in eine schriftlich fixierte Ordnung (sfO) zu bringen. Davon profitiert das gesamte Unternehmen.

In 14 Schritten zur ISO-27001-Zertifizierung

Bei der Etablierung eines ISMS nach ISO 27001:2013 sind die nachfolgenden 14 Themenbereiche zu behandeln.

Wichtig: Bei diesen Themenbereichen ist insbesondere darauf zu achten, dass alles, was nicht geregelt, nicht dokumentiert und nicht überwacht wird, bei einer Zertifizierung regelmäßig als „nicht vorhanden" bewertet wird. Dies unabhängig von der tatsächlichen Umsetzung einer technischen oder organisatorischen Sicherheitsmaßnahme. Sie müssen demnach sehr viel Augenmerk auf Dokumentationen und Kon-

trollnachweise legen. Das ist in der Regel eine neue Sichtweise für die Mitarbeiter. Gerade in IT-Abteilungen stoßen solche Dokumentationsanforderungen erfahrungsgemäß auf wenig Gegenliebe. In der IT-Abteilung wird eher lösungsorientiert gehandelt und nicht dokumentiert oder kontrolliert.

Schritt #1: So legen Sie den Geltungsbereich für Ihr ISMS fest

Eine der ersten Aufgaben bei der Implementierung eines ISMS ist die Festlegung des konkreten Geltungsbereichs (engl.: scope) des Managementsystems sowie die Durchführung einer Anforderungs- und Umfeldanalyse im Hinblick auf die Organisation und deren Stakeholder. Da die Festlegung des Geltungsbereichs der erste und entscheidende Schritt für den Aufbau und Betrieb des ISMS ist, sollte diese Phase besonders sorgfältig durchgeführt werden.

Die **Umfeldanalyse** enthält neben den für das ISMS relevanten organisatorischen und technischen Schnittstellen insbesondere auch branchentypische und standorttypische Gegebenheiten. Hierbei müssen z. B. Schnittstellen zu anderen wichtigen Abteilungen wie Risikomanagement, Personalabteilung, Datenschutz, Revision und Recht betrachtet werden. Ebenso sind Beziehungen zu wichtigen Lieferanten und Dienstleistern zu berücksichtigen.

In der **Anforderungsanalyse** sind die für das ISMS wichtigen Interessengruppen (engl.: stakeholder) aufzuführen und welche Anforderungen diese an die Organisation und das Managementsystem haben. Die Anforderungen können gesetzliche Vorgaben (z. B. BDSG, UWG, KRITIS, DSGVO, Regulierungsbehörden), aber auch vertragliche Verpflichtungen beinhalten.

Den richtigen Kontext zu schaffen ist für alle weiteren Schritte (z. B. Aufbau und Ablauf der Risikoanalyse, Organisationsstruktur, Definition von Arbeitspaketen und deren Priorisierung, Projektplanung) von zentraler Bedeutung. Dies auch für die Abschätzung der Machbarkeit und des Aufwands (Ressourcen, Budget, Zeit) für die Einführung des ISMS im Unternehmen.

Mein Tipp: Sie sollten als Geschäftsführer oder ISB den Scope des ISMS sehr genau planen und festlegen. In der Praxis hat sich oftmals gezeigt, dass ein falscher Scope zu erheblichen Kosten und Aufwänden führen kann. Sie sollten sich daher auf den Schutz Ihrer „Kronjuwelen" beschränken. Das spart Aufwand und Kosten.

Mit diesem 10-Punkte-Check holen Sie die Geschäftsführung ins Boot

Ein sachgerechtes ISMS wird im Top-down-Ansatz eingeführt und stellt einen Bezug zwischen den wirtschaftlichen Zielen des Unternehmens und der Informationssicherheit her. Dazu müssen zum einen die Anforderungen der Stakeholder berücksichtigt und zum anderen die auf Informationssicherheitsrisiken auf ein für das Unternehmen tragfähiges Maß reduziert werden.

Spätestens bei der Anpassung oder Neugestaltung von Prozessen muss die Führungsebene eingebunden werden. Denn ohne deren Unterstützung werden die Richtlinien und Änderungsprozesse keinen Rückhalt im Unternehmen haben. Daher wird explizit gefordert, dass die Unternehmensleitung und Führungskräfte nachweislich die Gesamtverantwortung für das ISMS übernehmen. Dies erfolgt regelmäßig durch die Veröffentlichung einer Informationssicherheitsleitlinie, die von der Geschäftsleitung in Kraft gesetzt wird. Die Veröffentlichung dieser Leitlinie zur Informationssicherheit entlässt die Unternehmensleitung aber nicht aus ihrer Verantwortung. Im Gegenteil: Alle Führungskräfte müssen ein sichtbares Engagement und ein klares Bekenntnis zur Informationssicherheit nachweisen können. Mit der nachfolgenden Checkliste können Sie prüfen, ob Ihre Führungskräfte und das Topmanagement diesen Anforderungen gerecht werden.

Checkliste „Führung und Engagement“ ISMS		
Anforderung	**Ja**	**Nein**
Halten die Führungskräfte die Anforderungen der Informationssicherheit ein (Vorbildfunktion)?	☐	☐
Stellen die Führungskräfte die zur Umsetzung der Anforderungen erforderlichen Ressourcen in ihren Verantwortungsbereichen bereit?	☐	☐
Werden Verstöße gegen die Leitlinien konsequent verfolgt?	☐	☐
Haben sich die Führungskräfte auf den „kontinuierlichen Verbesserungsprozess“ (KVP) verpflichtet?	☐	☐
Übernimmt das Topmanagement die Gesamtverantwortung für das ISMS?	☐	☐
Sind die Grundsätze zum Risikomanagement definiert und in Prozesse eingebunden?	☐	☐
Sind die Anforderungen der Informationssicherheit wirksam in alle Geschäftsprozesse und Projekte integriert?	☐	☐
Werden regelmäßig ISMS-Reviews im Topmanagement durchgeführt (Wirksamkeit, Sachgerechtigkeit usw.)?	☐	☐
Werden die erforderlichen Ressourcen zum Aufbau und zur Umsetzung des ISMS bereitgestellt?	☐	☐

Diese Maßnahmen stellen gerade bei der Einführung des ISMS hohe Anforderungen an das Topmanagement und die Führungskräfte. Werden diese Maßnahmen jedoch nicht umgesetzt, ist jedes ISMS zum Scheitern verurteilt. In solchen Projekten wird dann sehr viel Geld „verbrannt".

Schritt #3: KPIs für Ihr ISMS: Legen Sie messbare (!) Ziele fest

Das ISMS muss die Geschäftsziele unterstützen. Daher müssen die Ziele des ISMS klar von diesen abgeleitet und festgelegt werden. Dabei müssen die Ziele angemessen und auch messbar sein. Die Sicherheitsziele sollten langfristig angelegt sein und nicht konkret umzusetzende Sicherheitsmaßnahmen beschreiben. Typische Ziele der Informationssicherheit sind:

- Schutz vertraulicher Informationen des Unternehmens, der Kunden und Partner.
- Angemessene Verfügbarkeit und Integrität sämtlicher Geschäftsprozesse und der diese unterstützenden Unternehmenswerte (Assets)

- Erhaltung der in Geschäftsprozessen, Informations-Assets, IT-Assets und unterstützenden Assets investierten Werte
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen
- Sicherung der Qualität der Informationen – als Basis für eine korrekte Aufgabenabwicklung und geschäftssteuernde Entscheidungen
- Gewährleistung der aus gesetzlichen und regulatorischen Vorgaben resultierenden Anforderungen
- Sicherstellung der Kontinuität der Prozessabläufe
- Reduzierung der im Schadensfall entstehenden Aufwände

Die Messbarkeit der IS-Ziele ist in der Norm nicht zwingend vorgeschrieben, aber für die Überprüfung der Wirksamkeit des ISMS durchaus sinnvoll. Mögliche KPIs können z. B. die Anzahl der Betriebsunterbrechungen durch Cyberangriffe, die Anzahl der Datenpannen oder die Anzahl der Prozessunterbrechungen sein.

Schritt #4: Der Schlüssel zum Erfolg: Ihre Informationssicherheitsrichtlinie

Die Informationssicherheitsleitlinie ist ein wichtiges Werkzeug für das Unternehmen und steht an der Spitze der für das ISMS erforderlichen Dokumentenpyramide. In der IS-Leitlinie sind die wesentlichen strategischen und taktischen Ziele verankert, die mithilfe des ISMS erreicht werden sollen. Ebenso sollten die im ISMS benötigten Rollen und deren Aufgaben beschrieben werden. Sinnvoll ist es auch, die Funktionsträger oder Bereiche im Unternehmen zu benennen, die für die einzelnen Rollen verantwortlich sind.

Entscheidend für den Umsetzungserfolg und die Identifikation der Mitarbeiter mit dem Thema „Informationssicherheit“ ist, dass sich die Leitlinie sichtbar an den vorhandenen Unternehmens- und IT-Zielen orientiert und die Kernaussagen beim Leser einen Wiedererkennungseffekt zur eigenen Organisation hervorrufen. Das Abschreiben von Mustertexten ist in diesem Zusammenhang nicht zielführend.

Schritt #5: Taskforce „ISMS“: Stellen Sie Ihr Team zusammen

Die klare Definition von Zuständigkeiten und Befugnissen für Aufgaben, die für die Informationssicherheit relevant sind, ist von zentraler Bedeutung für die Wirksamkeit des ISMS und eine der Kernaufgaben der Unternehmensleitung. Hierbei sollte darauf geachtet werden, dass die Verantwortlichkeiten der Rollen klar geregelt und definiert sind und eventuelle Interessenkonflikte vermieden werden.

Typische Rollen im ISMS sind der Informationssicherheitsbeauftragte (ISB) oder Chief Information Security Officer (CISO), der Risikoeigentümer und der Asset-Eigentümer. In der IT-Sicherheit sind weitere Rollen wie z. B. Change Manager, Sicherheitsadministratoren, Auditoren usw. zu definieren. Hierbei sind Rollenkonflikte möglichst zu vermeiden. So sollte z. B. der ISB nicht gleichzeitig der IT-Leiter sein oder der ISM-Auditor gleichzeitig IT-Administrator. In beiden Fällen würden sich die Personen selbst überwachen bzw. kontrollieren. Der ISB sollte auch nicht Mitarbeiter der IT-Abteilung sein.

Für eine Zertifizierung ist es wichtig, dass die Rollen beschrieben und auch im Unternehmen verankert wurden. Dies kann z. B. in Stellenbeschreibungen, Arbeitsanweisungen oder Prozessdokumentationen erfolgen. Ebenso müssen Nachweise zur Qualifikation der jeweiligen Rollenträger im ISMS vorgelegt werden können.

Mein Tipp: Bei der Verteilung der Rollen sollte stets darauf geachtet werden, dass die Personen, die bereits über Erfahrungen in der IT-Sicherheit verfügen, auch im ISMS die entsprechenden Verantwortungsbereiche übernehmen. Neben den erforderlichen Fachkenntnissen sind hierbei Sozialkompetenzen sehr wichtig. Ohne gutes Kommunikationsverhalten, integres Auftreten, sachliche Überzeugungskraft und vor allem Konfliktmanagement sind viele der Aufgaben nicht zu lösen. Informationssicherheit bietet erhebliches Konfliktpotenzial und steht oftmals in Zielkonflikten mit weiteren Maßnahmen oder Funktionsträgern im Unternehmen. Ressourcenmangel, Prioritätskonflikte und Kosten sind die typischen Konfliktherde.

Schritt #6: Risikomanagement im ISMS: Decken Sie Schwachstellen auf, BEVOR etwas passiert

Ein wirksames Risikomanagement ist die Kernfunktion eines ISMS. Denn ohne ein funktionierendes Risikomanagement können die Sicherheitsziele des Unternehmens nicht erreicht werden. Das Risikomanagement verfolgt das Ziel zu analysieren, was alles passieren kann und was die möglichen Folgen sein können. Wobei ein Risiko die Abweichung von einem Erwartungswert darstellt. Im Risikomanagement ist es wichtig, Bedrohungen zu erkennen, diese in Bezug auf die Eintrittswahrscheinlichkeit und mögliche Schadenshöhen zu bewerten und daraus risikominimierende Maßnahmen zu entwickeln, die ein mögliches Schadenspotenzial auf ein akzeptables Niveau reduzieren. Wobei darüber, was als akzeptabel angesehen wird, die jeweiligen Risikoeigentümer unter Beteiligung der Asset-Eigentümer entscheiden müssen. Letztlich muss die Unternehmensleitung hierbei ihren Risikoappetit und damit den maximal tolerierbaren Schaden festlegen.

Die Prozesse „Informationsrisikomanagement“ (IRM) und „Informationssicherheitsmanagement“ sind zu unterscheiden. Das Sicherheitsmanagement führt, lenkt und koordiniert eine Organisation in Bezug auf alle Sicherheitsaktivitäten. Das Risikomanagement (RM) umfasst hingegen sämtliche Maßnahmen zur systematischen Erkennung, Analyse, Bewertung, Überwachung und Kontrolle von Risiken. Werden im Sicherheitsmanagement Schwachstellen, Abweichungen von Standards oder Fehler identifiziert, sind diese in das Risikomanagement zu überführen. Zur Steuerung der IT-Risiken ist es sinnvoll, diese den einzelnen ISO-Domains zuzuordnen. Das nachfolgende Schaubild zeigt eine beispielhafte Zuordnung.

Nr.	ISO Domain	Non-IT Risk	IT-Risk	Cyber-Risk
A.5	Informationssicherheitsrichtlinien	X		
A.6	Organisation der Informationssicherheit	X		
A.7	Personalsicherheit	X		
A.8	Verwaltung der Werte		X	
A.9	Zugangssteuerung		X	
A.10	Kryptographie			X
A.11	Physische und umgebungsbezogene Sicherheit	X		
A.12	Betriebssicherheit		X	
A.13	Kommunikationssicherheit			X
A.14	Anschaffung, Entwicklung und Instandhalten von Systemen		X	
A.15	Lieferantenbeziehungen	X		
A.16	Handhabung von Informationssicherheitsvorfällen	X		
A.17	Informationssicherheitsaspekte beim BCM	X		
A.18	Compliance	X		

4

Zuordnung von Risikokategorien zu ISO-Domains

Wobei das Sicherheitsmanagement insbesondere die Wirksamkeit der Prozesse:

- Berechtigungsmanagement
- IT-Projekte und Anwendungsentwicklung
- IT-Betrieb inkl. Datensicherung
- IT-Dienstleistungen

regelmäßig prüfen und Schwachstellen identifizieren muss. Insbesondere die Überwachung der IT-Dienstleister muss in der Regel intensiviert werden. Denn hier lauern erhebliche Risiken, die immer wieder zu schwerwiegenden Datenpannen und damit verbundenen hohen Schadenssummen führen.

Nur wenn diese Regelprozesse sachgerecht im Unternehmen umgesetzt werden, können Risiken minimiert werden und existenzbedrohende Schäden abgewehrt werden. Dies gilt angesichts der aktuellen Bedrohungslage insbesondere für Cyberrisiken.

Risiken der Informationssicherheit. Was ist darunter zu verstehen?

Risiken ergeben sich in der Informationssicherheit allein schon aus dem Nutzen von Informationstechnologien und regelmäßig aus aktuellen Bedrohungen, die auf Schwachstellen im Unternehmen abzielen. Daraus ergeben sich Eintrittswahrscheinlichkeiten und Schadenshöhen. Das Bundesamt für Sicherheit in der Informationstechnik hat im Jahr 2021 z. B. die nachfolgenden Top-10-Bedrohungen oder Risikoquellen für die Informationssicherheit identifiziert.

Die Top-10-Bedrohungen im Jahr 2021

1. Einschleusen von Schadsoftware
2. Infektion mit Schadsoftware über Internet und Intranet
3. Menschliches Fehlverhalten und Sabotage
4. Kompromittierung von Extranet und Cloud-Komponenten
5. Social Engineering und Phishing
6. (D)DoS-Angriffe
7. Internet-verbundene Steuerungskomponenten
8. Einbruch über Fernwartungszugänge
9. Technisches Fehlverhalten oder höhere Gewalt
10. Kompromittierung von Smartphones im Produktionsumfeld

Cybersicherheit: So unterstützt Sie ein 3-Lines-of-Defense-Modell im IRM

Das 3-Lines-of-Defense-Modell (3-LoD) dient der Förderung eines systematischen Ansatzes zur Identifikation und Handhabung von „Non financial Risks“ (NFR), gibt Leitlinien zur Ausgestaltung der Aufbauorganisation vor und regelt im Sinne einer Governance die Rollen und Verantwortlichkeiten der Verteidigungslinien.

Durch die heterogenen Wirkungsmechanismen und Verknüpfung der NFR werden die erste und zweite Verteidigungslinie für NFR in jeweils zwei Funktionen unterteilt, um einerseits in der spezialisierten 1-LoD eine unternehmensweite Steuerung des Risikoprofils von Einzelthemen zu ermöglichen, andererseits, um durch eine zentrale (bereichs-)übergreifende Verantwortlichkeit ein einheitliches Risikomanagement – trotz der heterogenen Einzelrisikoprofile – zu schaffen.

Quelle: ISB Andreas Hessel 05/2019

Non-Financial Risk Management (NFRM)

Cyberangriffe werden nicht nur häufiger, sondern auch immer raffinierter. Gleichzeitig steigt durch die Digitalisierung das Risiko, von solchen Angriffen betroffen zu sein. Auch stehen immer mehr Unternehmensbereiche –außerhalb der traditionell besonders gefährdeten Bereiche wie Verteidigung, Energie und Pharmazie – im Visier der Cyberkriminellen. Deshalb müssen sich Unternehmen heutzutage nicht fragen, ob, sondern wann sie Opfer eines Angriffs werden. Jedes zweite Unternehmen war in den vergangenen zwei Jahren von Cyberkriminalität betroffen. Der

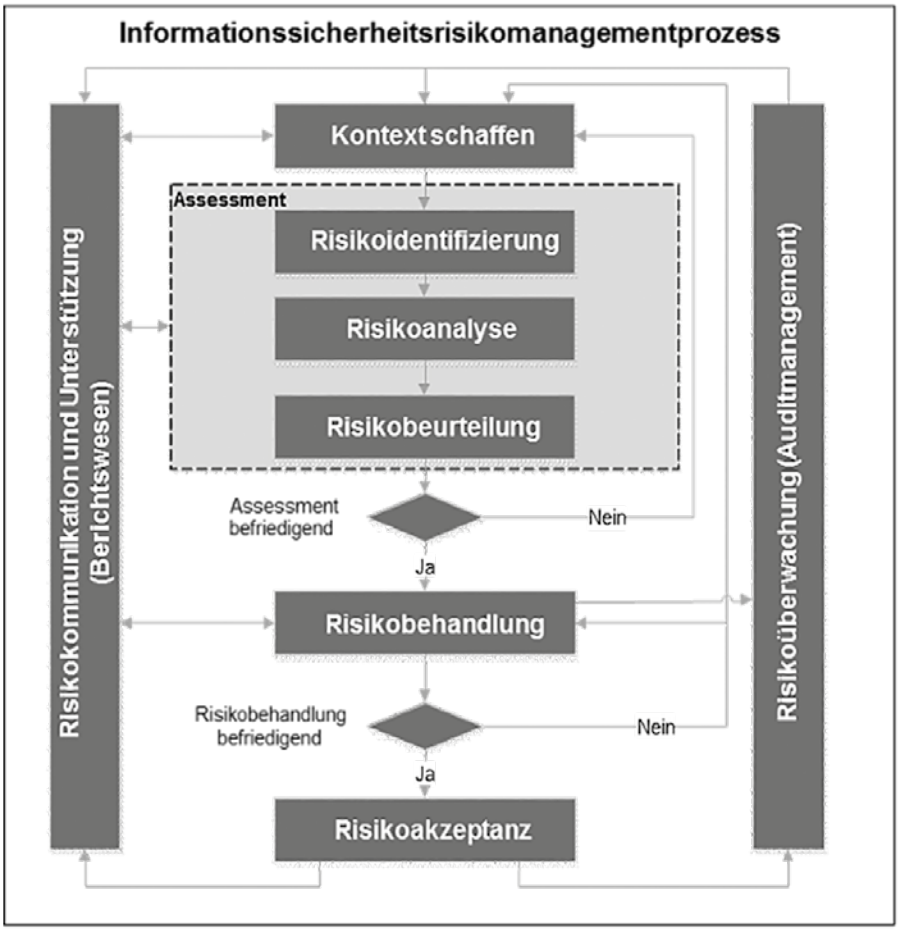
Aufbau sachgerechter Risikomanagementprozesse ist für das gesamte Unternehmen eine enorme Herausforderung. Müssen doch nahezu alle Unternehmensbereiche aktiv in diese Prozesse eingebunden werden.

Ein Unternehmen, das in der Lage ist, alle Risiken umfassend und auf Basis eines validen Geschäftsmodells schnell und richtig zu identifizieren und zu managen, kann dadurch mehr Geschäft generieren sowie Geschäftsausfälle besser vermeiden. In Anbetracht der aufgelaufenen enormen Verluste und Lösegeldzahlungen in den Jahren 2021 und 2022 können durch ein effektives NFRM-Framework Schäden in signifikanter Höhe vermieden werden. Zur Zukunft von NFRM stellt sich – speziell aufgrund der aktuellen Bedrohungslage – nicht mehr die Frage, „ob" gehandelt werden muss, sondern „wie und wann".

Das sind die konkreten Ziele des Risikomanagements im ISMS gem. ISO 27001:2013:

- Frühzeitiges Erkennen und Beheben von Informationssicherheitsrisiken
- Etablierung einheitlicher Bewertungsmethoden für identifizierte Risiken
- Eindeutige Zuweisung von Verantwortlichkeiten beim Umgang mit Risiken
- Standardisierte und übersichtliche Dokumentation von Risiken, inklusive deren Bewertungen
- Effiziente Behandlung von Risiken
- Regelmäßiges Berichtswesen an die Unternehmensleitung

Im Risikomanagement sind die nachfolgenden Prozesse zu durchlaufen:



Prozesse im Informationssicherheitsrisikomanagement.

Schritt #7: Erfolgsanalyse: Stellen Sie Ihr ISMS anhand der KPIs auf den Prüfstand

Ein ISMS muss sicherstellen, dass die Einhaltung der Vorgaben kontinuierlich überwacht wird und damit gewährleistet werden kann, dass die Sicherheitsziele des Unternehmens erreicht werden. Hierfür sind im ISMS Messverfahren und Key-Performance-Indikatoren (KPI) zu entwickeln. KPIs dienen dazu, grundlegende Aussagen über die Wirksamkeit und Sachgerechtigkeit des ISMS treffen und diese an die Unternehmensleitung berichten zu können. Ziel ist es demnach, ein sachgerechtes Steuerungsinstrument für die Geschäftsleitung zu entwickeln. Durch KPIs können sowohl Indizien auf (neue) Risiken bzw. Veränderungen innerhalb der Risikolandschaft als auch Nichtkonformitäten in Bezug auf die Umsetzung von Sicherheitsvorgaben und Richtlinien aufgedeckt werden. Die Entwicklung sachgerechter KPIs ist eine große Herausforderung und erfordert ein hohes Maß an Dokumentation in den Bereichen, in denen die Indikatoren laufen. Die ISO 27001:2013 legt dabei keine Indikatoren fest, sondern fordert mindestens die nachfolgende Dokumentation der Indikatoren:

- Wie sind die Metriken im Einzelnen definiert?
- Was wurde gemessen und bewertet?
- Welche Methoden zur Messung, Analyse und Bewertung wurden herangezogen und führen diese zu reproduzierbaren Ergebnissen?
- Wann wurde durch wen gemessen?
- Wann wurde durch wen analysiert und bewertet?

Mein Tipp: Bevor Sie sich mit KPIs beschäftigen, sollten Sie alle anderen Maßnahmen zur Etablierung eines ISMS umgesetzt haben. Erst wenn diese Prozesse im Unternehmen etabliert sind und zumindest stabil funktionieren, sollten Sie sich mit KPIs beschäftigen. Sie müssen dabei bedenken, dass Sie alle Bereiche zunächst dazu befähigen müssen, überhaupt die geforderten Dokumentationen erstellen zu können. Dazu sind ein hohes Maß an Standardisierung, Motivation und konsequentes Handeln erforderlich, das in den meisten Abteilungen in der erforderlichen Qualität zu Beginn noch nicht vorhanden ist.

Schritt #8: Dokumentation nach ISO 27001: Mit dieser Checkliste prüfen Sie Ihr Sicherheitslevel

Die Anforderungen an die Dokumentation sind in der ISO 27001:2013 sehr hoch. Das stellt viele Unternehmen vor enorme Herausforderungen. Gerade kleine und mittelständische Unternehmen verfügen regelmäßig nicht über umfangreiche Dokumentationen der Betriebsabläufe oder Prozesse, Richtlinien, Arbeitsanweisungen, Betriebshandbücher in der IT usw. Letztlich fehlt oftmals eine vollständige schriftlich fixierte Ordnung (sfO) inklusive regelmäßiger Aktualisierungs- und Freigabeprozesse. Dabei sind mindestens nachfolgende Aspekte zu regeln:

- Die Erstellung und Aktualisierung sowie die Genehmigung bzw. Freigabe durch Kompetenzträger und ggf. Veröffentlichung von Dokumenten müssen nach einem definierten Verfahren (Workflow) erfolgen.

- Es muss eine eindeutige Kennzeichnung von Dokumenten stattfinden, z. B. Titel, Datum, Autor, Version, Ablage sowie eine angemessene Qualitätskontrolle (Inhalt und Form) und abschließende Freigabe.
- Klassifizierung der Dokumente bzw. deren Inhalte bzgl. der Vertraulichkeit
- Erstellung ausreichender und inhaltlich relevanter Aufzeichnungen im Rahmen der operativen Tätigkeiten zur Sicherstellung der Nachvollziehbarkeit (Handbücher, Betriebs- und Sicherheitskonzepte usw.).

Neben der Erstellung der Dokumente muss auch Sorge dafür getragen werden, dass diese Dokumente im Unternehmen allen Mitarbeitern bekannt gemacht werden. Weitere Aspekte zur Einschätzung der Qualität der Dokumentationen und der Dokumentenlenkung können Sie mit der nachfolgenden Checkliste ermitteln:

Checkliste „Dokumentationen“:		
Anforderung	**Ja**	**Nein**
Sind die Mitarbeiter mit den Inhalten vertraut und werden die Anforderungen der Dokumente von den Betroffenen im Alltag „gelebt“?	☐	☐
Kennen die Mitarbeiter die Ablageorte und Medien, an/in denen die aktuellen Dokumente zu finden sind?	☐	☐
Sind die Inhalte zielgruppenorientiert aufbereitet und eindeutig formuliert?	☐	☐
Können neue Mitarbeiter die Inhalte der Dokumente erfassen und in ihrem Arbeitsumfeld umsetzen?	☐	☐
Gibt es regelmäßige Nachfragen der Mitarbeiter zu einzelnen Dokumenten?	☐	☐
Werden die Dokumente regelmäßig (mindestens jährlich) bzw. auf Aufforderung aktualisiert?	☐	☐
Wird der Aktualisierungs- und Freigabeprozess problemlos durchlaufen?	☐	☐
Sind für jeden Dokumententyp Eigentümer festgelegt?	☐	☐

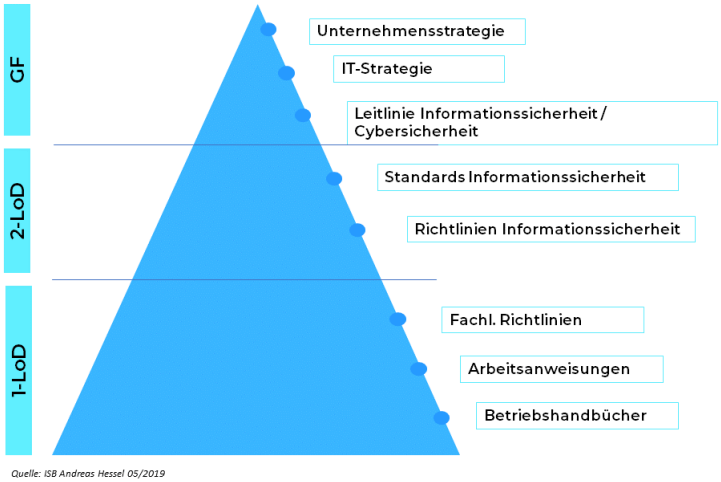
Jede Anforderung sollte mit einem Ja beantwortet werden. Andernfalls müssen geeignete Maßnahmen zur Umsetzung der Anforderung getroffen werden.

Mit der nachfolgenden Checkliste können Sie Mindestanforderungen an die Vollständigkeit Ihrer Dokumentationen prüfen:

Checkliste „Vollständigkeit der Dokumentationen“:		
Dokumentation	**Ja**	**Nein**
Geltungsbereich des ISMS beschrieben?	☐	☐
Informationssicherheitsleitlinie erstellt?	☐	☐
Prozesse im Risikomanagement beschrieben (Risikobeurteilung, Risikobehandlung)?	☐	☐
Erklärung zur Anwendbarkeit der Risikoprozesse erstellt?	☐	☐
Risikobehandlungsplan erstellt?	☐	☐
Sicherheitsziele definiert?	☐	☐
Kompetenznachweise dokumentiert?	☐	☐
Nachweise zur korrekten Ausführung der Prozesse im ISMS erstellt?	☐	☐
Ergebnisse der Risikobeurteilung und Risikobehandlung dokumentiert?	☐	☐
Kontroll- und Leistungsmessungen (KPI) nachweislich dokumentiert?	☐	☐
Durchführung von Audits und deren Resultate dokumentiert?	☐	☐
Ergebnisse der Management Reviews dokumentiert?	☐	☐
Abweichungen von ISMS-Vorgaben und deren Behandlung dokumentiert?	☐	☐
Fortlaufende Korrekturmaßnahmen (KVP) dokumentiert?	☐	☐

Sie müssen zu jedem dieser Punkte eine fortlaufende und nachweisliche Dokumentation führen. Zudem müssen Sie die entsprechenden Prozessbeschreibungen dokumentieren.

Eine typische Dokumentenpyramide für eine schriftlich fixierte Ordnung kann wie folgt aufgebaut werden:



Dokumentenpyramide für eine schriftlich fixierte Ordnung

Schritt #9: Kommunizieren Sie Ihre Maßnahmen – nach innen und nach außen

Die wesentliche Anforderung im Baustein „Kommunikation“ besteht darin, die Schnittstellen zu anderen internen Bereichen wie z. B. IT-Abteilung, Personal, Revision, Datenschutz, Risikomanagement zu beschreiben und einen regelmäßigen Informationsaustausch zu initiieren. Aber auch die Kommunikation mit externen Stellen wie Dienstleister, Behörden usw. ist zu beschreiben.

Sie müssen ebenso Berichtswege zu den definierten internen und externen Stellen festlegen und regelmäßig dokumentieren. In der Praxis sollten Sie regelmäßige Meetings mit den Stakeholdern im Unternehmen durchführen und diese Meetings in Ergebnisprotokollen dokumentieren. An die Unternehmensführung sollten Sie als ISB regelmäßig mindestens halbjährlich berichten. Diese Berichte sollten über den Stand des ISMS und die Risikosituation im Unternehmen informieren.

Mit den Dienstleistern sollten Sie einmal jährlich einen Austausch über den Stand ihrer ISMS und deren Anforderungen durchführen. Von den Dienstleistern sollten Sie dazu jährliche Berichte über den Stand des ISMS anfordern und Schwachstellen ggf. in Ihr Risikomanagement überführen.

Mein Tipp: Unterschätzen Sie nicht die hohen Risiken, die sich aus Abhängigkeiten zu Dienstleistern ergeben. Schwachstellen in deren ISMS können sehr schnell zu Ausfällen in der Lieferkette oder zu Datenverlusten führen. Insbesondere beim Outsourcing von IT-Dienstleistungen sind die Risiken in der Regel hoch. Hier müssen Sie regelmäßige Prüfungen und Audits durchführen und diese auch dokumentieren.

Schritt #10: Der große Awareness-Check: Machen Sie Mitarbeiter in Sachen IT-Sicherheit fit!

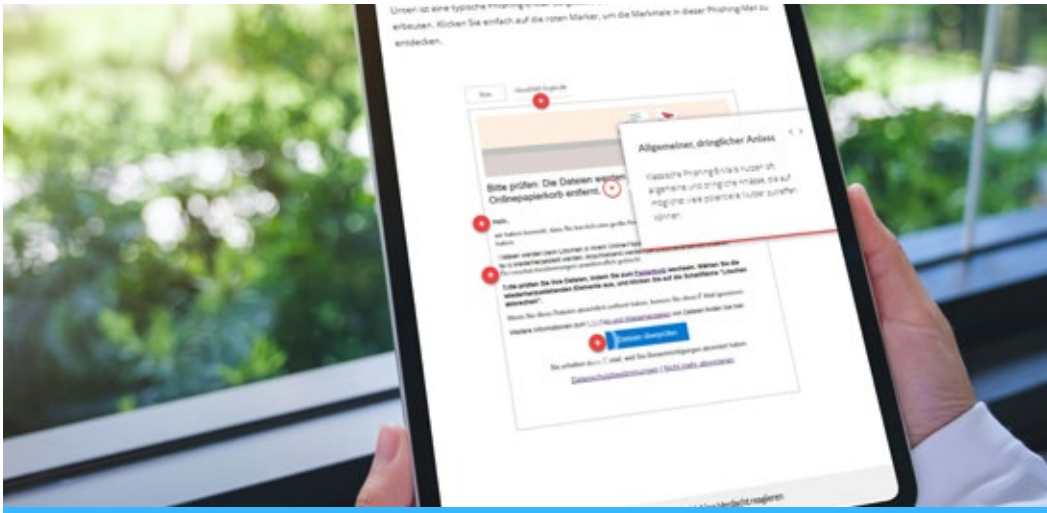
Angesichts der aktuellen Bedrohungslage durch Cyberkriminelle ist es für Unternehmen äußerst wichtig, die Mitarbeiter zu den zentralen Themen der Informationssicherheit zu sensibilisieren und eine wirksame Security Awareness aufzubauen. Mitarbeiter müssen eine aktive Haltung gegenüber Bedrohungen einnehmen. Dies ist nur zu erreichen, wenn Sie als Geschäftsführer oder ISB aktiv für die Etablierung einer Sicherheitskultur in Ihrem Unternehmen eintreten.

Je weniger sich ein Mitarbeiter oder eine Führungskraft der konkreten Risiken bewusst ist, mit denen er oder sie tagtäglich konfrontiert ist, und je weniger die geltenden Sicherheitsvorgaben und Prozesse bei den jeweils Betroffenen bekannt sind, desto schwieriger wird es, das angestrebte Sicherheitsniveau im Unternehmen zu erfüllen und transparent zu ma-

chen. Die Schaffung eines nachhaltigen Risikobewusstseins ist daher ein wesentlicher Bestandteil eines praxistauglichen ISMS. Der Nutzen für Ihr Unternehmen besteht darin, dass Bedrohungen frühzeitig erkannt, Sicherheitsvorfälle vermieden und die Aufwände, die für deren Behandlung notwendig wären, eingespart werden können.

Sie müssen im Unternehmen demnach regelmäßige Schulungen und Sensibilisierungsmaßnahmen durchführen, um die Security Awareness Ihrer Mitarbeiter zu erhöhen. Erstellen Sie dazu einen jährlichen Schulungsplan mit Themen und Maßnahmen wie z. B. einer Awareness-Kampagne. Dokumentieren Sie die Schulungsmaßnahmen und lassen Sie die Teilnehmer Tests durchführen. An dieser Stelle sind wieder KPIs sinnvoll. Sie sollten messen, wie viele Mitarbeiter die Schulungen erfolgreich durchlaufen haben und wie die Resonanz der Teilnehmer war (Umfrage).

Eine der häufigsten Angriffsmethoden der Cyberkriminellen sind gefälschte E-Mails mit Malware (Trojaner, Ransomware usw.) oder Phishing-Methoden (Ausspähen von Passwörtern usw.). Solche Angriffe können mittels Phishing-Simulationen sehr wirkungsvoll abgewehrt werden. Die Wirksamkeit solcher Phishing-Simulationen ist wissenschaftlich belegt. Davon können Sie auch in Ihrem Unternehmen profitieren.



So bauen Sie eine wirksame Awareness-Kampagne auf (Bitte keinen Schritt überspringen!)

Jeder einzelne Schritt Ihrer Awareness-Kampagne muss durchgeführt werden, um den gewünschten Effekt zu erzielen. Kein Schritt darf übersprungen werden. (Wir von CyberXperts unterstützen Sie dabei gerne. Mehr Informationen.)

Planen Sie deshalb diese Bestandteile Ihrer Kampagne ein:

Schritt 1: Mit guter Vorbereitung legen Sie den Grundstein für Ihren Erfolg

- Definieren Sie Ihre Ziele ganz klar – oder lassen Sie es gleich bleiben!
- Der Slogan: Das zentrale Element Ihrer Kampagne
- Ihr wichtigster Verbündeter: Die Geschäftsleitung

Schritt 2: Versenden Sie die (Fake-)Phishing-Mail – OHNE Ankündigung!

Schritt 3: Jetzt lösen Sie auf … und starten Ihre Sensibilisierungs-Kampagne

- Lassen Sie die Geschäftsleitung den Start der Kampagne einläuten (Management-Attention)
- Präsentieren Sie jetzt Ihre Ergebnisse: *„Leute, Ihr habt da auf einen Phishing-Link geklickt … das muss besser werden!“*
- Kampagne mit Werbeträgern (Plakate, Flyer, Intranetseite usw.)
- Zielgruppenorientierte Trainings: So erreichen Sie die Mitarbeiter
- Webbased-Training: Mit spannenden E-Learnings schaffen Sie Awareness
- 20 Minuten Training für die Führungskräfte – So werden sie zu Vorbildern und Multiplikatoren

Schritt 4: Messen Sie den Erfolg anhand dieser Kriterien

Wollen auch Sie sich Ihre nächste Awareness-Kampagne besonders einfach machen?

CyberXperts unterstützt Sie bei jedem der 4 Schritte. Unsere netten Berater zeigen Ihnen gerne, welche genialen Möglichkeiten Sie mit CyberXperts haben. Einfach hier Strategie-Beratungsgespräch ausmachen.

Andreas Hessel
Chief Information Security Officer

Naomi Meier
Senior Sales Managerin

Schritt 1: Mit guter Vorbereitung legen Sie den Grundstein für Ihren Kampagnen-Erfolg

Definieren Sie Ihre Ziele ganz klar – oder lassen Sie es gleich bleiben!

Eine Awareness-Kampagne kann nur erfolgreich sein, wenn die Ziele konkret definiert sind. Andernfalls werden Sie bei den Mitarbeitern das Gefühl von Beliebigkeit erzeugen, aber Sie werden niemanden begeistern können.

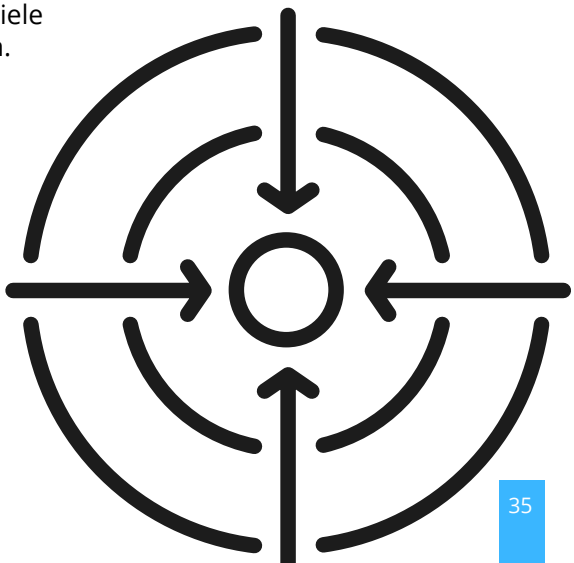
Ohne konkrete Ziele ist der Erfolg einer Awareness-Kampagne auch nicht messbar.

Konkret könnten Sie sich beispielsweise das Ziel setzen, die Mitarbeiter zu den folgenden Themen zu sensibilisieren:

- Social Engineering
- Trojaner und Ransomware
- E-Mail-Sicherheit

Sie möchten zudem den Erfolg der Awareness-Kampagne messen und dauerhaft wirksame Maßnahmen zur Etablierung einer Sicherheitskultur etablieren.

Tipp: Wir entwickeln die Ziele gerne gemeinsam mit Ihnen. Besprechen Sie Ihre Ziele einfach mit unseren CyberXperts-Kundenbetreuern. Falls Sie sich unsicher sind, welche Ziele möglich oder sinnvoll sind, beraten diese Sie gerne. Völlig unverbindlich. Hier kostenlos persönliches Gespräch reservieren.



Der Slogan: Das zentrale Element Ihrer Kampagne

Eine Awareness-Kampagne benötigt zunächst einen aussagekräftigen Slogan und, falls möglich, ein Logo.

Beide Elemente sollten so gewählt werden, dass sie zur Corporate Identity (CI) Ihres Unternehmens passen und auf Ihren Veröffentlichungen (Rundschreiben, E-Mails, Intranetseiten) verwendet werden können.

So erreichen Sie einen dauerhaften Wiedererkennungseffekt, der auch dazu führt, dass die Inhalte der Kampagne bei den Mitarbeitern in Erinnerung bleiben.

Mein Tipp: Mit einem Slogan erreichen Sie Mitarbeiter. Sie signalisieren ihnen, dass Ihr Unternehmen die Mitarbeiter wertschätzt und auf sie baut. So verhindern Sie Trotz-Reaktionen und gehen gleichzeitig gegen die Beharrlichkeit einiger Kollegen vor. Setzen Sie sich mit Ihrer Marketingabteilung in Verbindung. Die Kollegen kennen bestimmt einen Grafiker, der Ihnen zu Ihrem Slogan ein Logo entwirft.

Konkrete Beispiele zu Slogans:

„Sie sind der wichtigste Mitarbeiter der IT-Sicherheit."

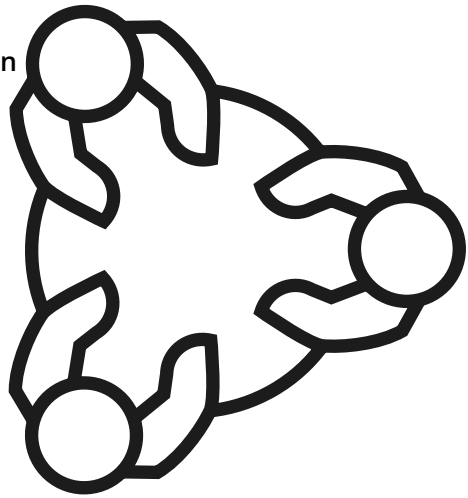
„Unsere Mitarbeiter sind unsere stärkste Firewall."

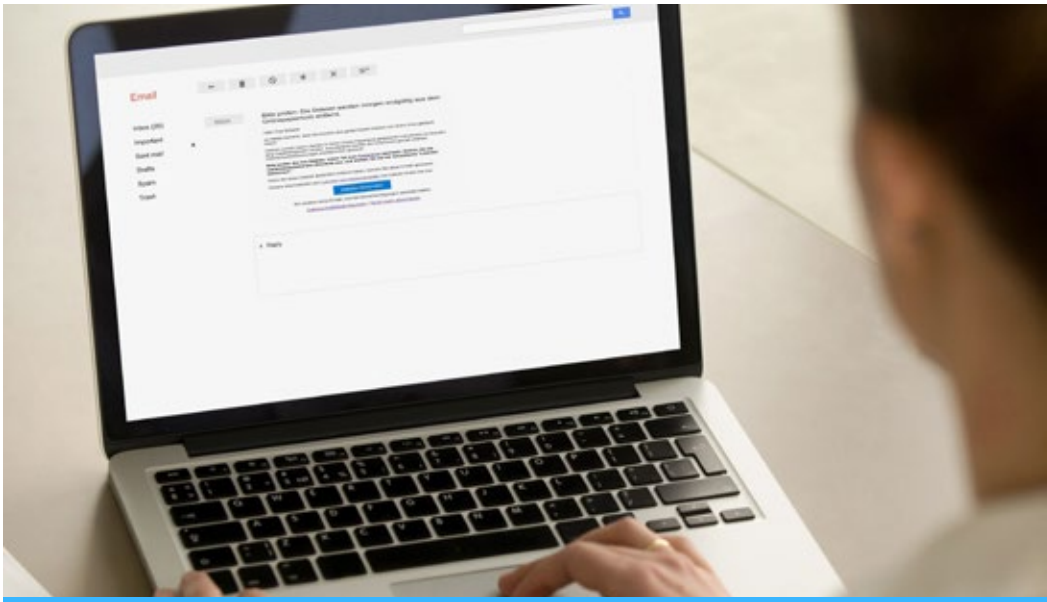
„Sie trotzen jedem Angriff. Mit SICHERHEIT."

Ihr wichtigster Verbündeter: Die Geschäftsleitung

Sie müssen bei der Planung einer Awareness-Kampagne vieles beachten. Zunächst sollten Sie sich darüber im Klaren sein, dass eine solche Kampagne ohne die Unterstützung der Geschäftsleitung nicht sinnvoll ist. Nur wenn Ihre Geschäftsleitung sich klar und deutlich zu den Inhalten der Awareness-Kampagne bekennt und Sie unterstützt, können Sie beginnen.

Jetzt haben Sie Ihre Geschäftsleitung davon überzeugt, dass eine Security-Awareness-Kampagne für die Sicherheit im Unternehmen unerlässlich ist. Sie haben ein Budget, mit dem Sie zumindest die begleitenden Maßnahmen wie Flyer, Plakate, usw. finanzieren können. Bestenfalls haben Sie noch ein Budget für externe Unterstützung durch versierte Berater.





Schritt 2: Versenden Sie eine (Fake-)-Phishing-Mail – OHNE Ankündigung!

In Ihrem Unternehmen ist von Ihren Planungen noch nichts bekannt geworden.

Das sollte auch so bleiben. Denn jetzt müssen Sie den Paukenschlag vorbereiten, mit dem Sie Ihre Kampagne starten. Damit dieser Start gelingt, müssen Sie die volle Aufmerksamkeit Ihrer Mitarbeiter haben.

Als Paukenschlag hat sich bewährt, einen Phishing-Angriff per E-Mail nachzubilden.

Achtung: Diese Kollegen müssen trotzdem VORHER informiert werden! Bevor Sie Ihren „Angriff" per E-Mail starten, müssen Sie sicherstellen, dass Datenschutzbeauftragte und IT-Sicherheitsbeauftragte an einem Strang ziehen und den Betriebsrat informieren. Die Kollegen aus der IT müssen darauf vorbereitet sein, dass Mitarbeiter beim Support nachfragen, was denn das für eine E-Mail sei usw. Den Betriebsrat müssen Sie darüber informieren, dass Sie lediglich Aufmerksamkeit für die Kampagne erreichen wollen, dass ausschließlich anonymisierte Daten gespeichert werden und keine personenbezogenen Auswertungen gemacht werden.

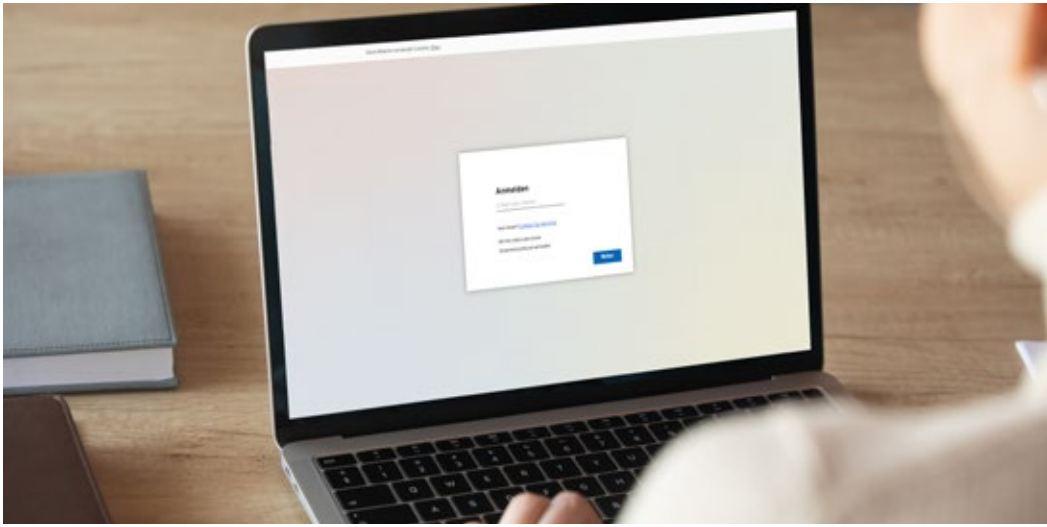
Wie Sie Ihre Phishing-Mail so richtig echt wirken lassen

Hierzu müssen Sie sich zunächst ein Szenario ausdenken, mit dem Sie die Mitarbeiter ködern können. Versuchen Sie, ein realistisches Szenario zu finden, das zu Ihrem Unternehmen passt.

Bereiten Sie z. B. eine E-Mail vor, in der Sie nachfolgendes Szenario beschreiben: Im Unternehmen sollen iPhones eingeführt werden. Die IT-Abteilung sucht nun Mitarbeiter, die bereit sind, die neuen Geräte auf Herz und Nieren zu testen. Die Testpersonen können die iPhones als Dankeschön am Ende des Tests behalten. Da nur eine begrenzte Anzahl von Testgeräten bereitsteht, werden die Teilnehmer ausgelost. Die Interessenten müssen sich auf der Internetseite des Unternehmens mit ihrem Benutzeraccount und Passwort registrieren.

Im nächsten Schritt müssen Sie eine **Internetseite bereitstellen, die das oben aufgeführte Szenario abbildet.**

Auf dieser Seite muss ein Eingabefeld für einen Benutzernamen und ein Passwort vorhanden sein. Die Anzahl der Besucher der Internetseite und die Anzahl der Mitarbeiter, welche die Anmeldung durchgeführt haben, muss gespeichert werden.

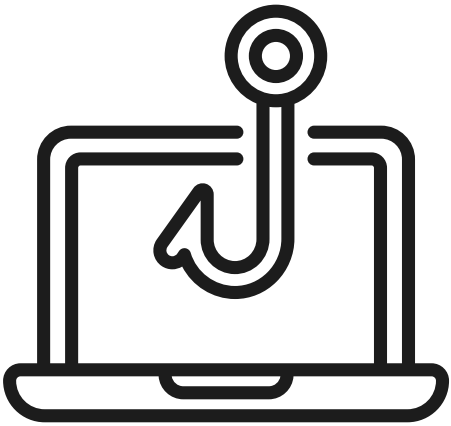


Benutzen Sie einfach diese Fix und fertige Phishing-Simulation

Wenn Sie den Aufwand der Erstellung von E-Mail und dazugehöriger Internetseite nicht leisten wollen oder können, bietet sich CyberXperts als perfekte Lösung an:

Denn CyberXperts bietet für Ihre Phishing-Simulation bereits **fertige Lösungen, die individuell auf Ihr Unternehmen abgestimmt werden. So sparen Sie sich viel Aufwand!** Wir kümmern uns um die Erstellung der Mails, Versand und Auswertung Ihrer Kampagne. Hier mehr Informationen erhalten.

Jetzt gratis Phishing-E-Mails zu Programmen wie Microsoft Teams, Outlook oder Cloud-Anbietern erstellen! Direkt hier Ihren persönlichen Beratungstermin vereinbaren.



Nur mit maximalem Schock-Effekt erzielen Sie eine Verhaltensänderung

Wenn die E-Mail sprachlich zu Ihrem Unternehmen passt und sich inhaltlich auf ein reales allgemein bekanntes Thema bezieht, werden in der Regel die meisten Mitarbeiter in die Falle tappen.

Instruieren Sie die IT: Machen Sie den Kollegen klar, dass sie den Mitarbeitern, die sich über die Hintergründe der E-Mail informieren wollen, keine direkten Auskünfte zu der Kampagne geben. Natürlich dürfen sie auch nicht bestätigen, dass die E-Mail echt ist. Am besten ist es, wenn die Kollegen des IT-Supportes einfach aussagen, dass sie die Hintergründe klären müssen, und sich dann wieder melden. Für die Statistik ist es wichtig, dass die Anzahl der Anrufer festgehalten wird. Weisen Sie darauf hin, dass keine Namen registriert werden dürfen. Nach diesen Vorbereitungen können Sie die E-Mail an alle Mitarbeiter senden.

Tipp: Werten Sie die Ergebnisse am gleichen Tag aus. Dass mit dieser E-Mail irgendetwas nicht stimmt, wird sich schnell in Ihrem Unternehmen verbreiten. Nachzügler sind daher meist informiert und verfälschen das Bild.

Schritt 3: Jetzt lösen Sie auf … und starten Ihre Sensibilisierungs-Kampagne offiziell

Lassen Sie die Geschäftsleitung den Start der Kampagne einläuten

Nach dem Versand der Phishing-E-Mail sollten Sie unmittelbar am darauffolgenden Tag mit der Kampagne starten. Lassen Sie die E-Mail der Geschäftsleitung daher auch am Vorabend versenden. In dieser E-Mail sollte die Geschäftsleitung die Kampagne kurz vorstellen, die gemeinsamen Ziele sowie die zentrale Rolle der Mitarbeiter hervorheben.

Präsentieren Sie jetzt Ihre Ergebnisse: *„Leute, Ihr habt da auf einen Phishing-Link geklickt … das muss besser werden!“*

Präsentationen zu Awareness-Kampagnen müssen zentrale Botschaften und kein Fachwissen vermitteln. Fachwissen wird in Trainingseinheiten vermittelt. Verwenden Sie daher in Ihren Präsentationen viel Bildmaterial, Comicfiguren, Videos und wenig Text.

Sie müssen die Mitarbeiter begeistern und nicht langweilen. Bewährt haben sich auch kleine Live-Hacking-Beiträge, bei denen z. B. gezeigt wird, wie schnell Passwörter gehackt werden oder wie leicht man mit einem USB-Stick Daten ausspionieren kann.

Auch das macht eine Kampagne mit CyberXperts für Sie besonders attraktiv:

CyberXperts wertet alle Phishingkampagnen auf Abteilungsebene für Sie aus und erstellt passende Grafiken, mit denen Sie Ihre Mitarbeiter überzeugen können. Spannende E-Learnings inkl. Videos unterstützen Sie bei der Präsentation in Ihrem Unternehmen. Jetzt gratis Beratungstermin für Ihre erste Phishing-Simulation vereinbaren!

Tipp: Zu den Präsentationsterminen sollten alle Mitarbeiter eingeladen werden. Wirken Sie darauf hin, dass die Geschäftsleitung vor jeder Präsentation zu den Mitarbeitern spricht und sich für die Ziele der Awareness-Kampagne stark macht. Die Anwesenheit des Managements ist für den Erfolg der Awareness-Kampagne von entscheidender Bedeutung. Das lockert die Stimmung auf und sorgt für Solidarität mit den Mitarbeitern.

Diese Inhalte sollte Ihre Präsentation haben:

- **Stellen Sie die Ergebnisse der Phishing-E-Mail dar.** Heben Sie hervor, wie viel Prozent der Mitarbeiter den Link in der Mail angeklickt haben und wie viele Mitarbeiter tatsächlich ihren Benutzernamen und ihr Passwort eingegeben haben.
- **Weisen Sie aber darauf hin, dass dieses Ergebnis normal ist.** Verdeutlichen Sie, dass es menschlich ist, seiner Neugierde nachzugeben und solchen vermeintlich attraktiven Angeboten reflexartig nachzukommen.
- **Vermeiden Sie den Oberlehrer** und weisen Sie darauf hin, dass Sie auch schon in solche Fallen getappt sind. So können Sie die Mitarbeiter sensibilisieren und in die Awareness-Kampagne mitnehmen.

Denken Sie immer daran, dass Sie gegen Beharrlichkeit und Trotz der Mitarbeiter kämpfen müssen. Da hilft es nicht, mit Fachwissen zu glänzen. Ein Lacher und ein gut gemachtes Video (das Sie z. B. bei CyberXperts finden), das die Zuschauer fesselt, sind bei weitem hilfreicher.

Zielgruppenorientierte Trainings: So erreichen Sie die Mitarbeiter

Sie haben die Mitarbeiter mit Ihrer Phishing-Mail aufgerüttelt und die Ergebnisse gezeigt. Ihre Security-Awareness-Kampagne war ein voller Erfolg. Nun gilt es, diese Aufmerksamkeit zu nutzen, um den Mitarbeitern Ihre zentralen Themen nachhaltig zu vermitteln.

Um dieses Ziel zu erreichen, führen Sie zielgruppenorientierte Trainings durch. Zielgruppen sind in der Regel „alle Mitarbeiter", „Führungskräfte" und „Geschäftsleitung".

Neben diesen primären Zielgruppen sollten Sie Trainings zu speziellen Business-Themen oder Abteilungen planen wie z. B. Personaldaten, Kundendaten, Forschungsdaten sowie Ergänzungstrainings zu Sicherheitsthemen.

CyberXperts bietet Ihnen die **perfekten Vorlagen und Trainingsmaterialien** für Ihre Schulungen. Hier gratis informieren.

Webbased Training: Mit spannenden E-Learnings schaffen Sie Awareness

Für die Zielgruppe „Alle Mitarbeiter" können Sie nur in kleinen Unternehmen Präsenztrainings anbieten. Ab einer Größenordnung von 100 Mitarbeitern ist der Einsatz eines Webbased Trainings (WBT) sinnvoller.

Tipp: Das Training muss kurzweilig und interessant sein. Die Mitarbeiter müssen das WBT aufrufen, weil es ihnen Spaß macht. Nur so können Sie vermeiden, dass das WBT als lästige Pflichtübung verstanden wird und die Lösungen für die Testfragen im Unternehmen kursieren, weil jeder das WBT schnell durchklicken will. Ein langweiliges WBT oder ein WBT, in dem mit dem erhobenen Zeigefinger gearbeitet wird, kann Ihnen die Erfolge Ihrer gesamten Security-Awareness-Kampagne zunichtemachen.

In der Regel können diese Programme auf das Corporate Design des Unternehmens angepasst werden. Sie sollten die Slogans und Logos Ihrer Awareness-Kampagne in das WBT integrieren lassen. Achten Sie bei der Auswahl eines Produktes darauf, dass dabei mit Multimedia-Inhalten (Videos, Animationen, Comicelemente, Sprache usw.) gearbeitet wird und eine Erfolgskontrolle oder ein Test integriert ist.

Sie möchte Ihre Mitarbeiter mit spannenden E-Learnings inklusive interaktiven Elementen wie Videos oder Quiz sensibilisieren? **CyberXperts bietet eine große Auswahl an Awareness-Schulungen, die Ihre Mitarbeiter mit realen Beispielen wirksam schulen.** Hier gratis und unverbindlich informieren.

Tipp: Das WBT sollte einen Pool von Fragen bereitstellen und nach einem Zufallsprinzip eine bestimmte Anzahl von Fragen für den Teilnehmer auswählen. Das WBT sollte nicht länger als eine Stunde dauern und es muss die Möglichkeit bestehen, dass der Teilnehmer das WBT an beliebigen Stellen wiederaufnehmen kann. Der Teilnehmer muss auch den Test so lange wiederholen können, bis er alle Fragen beantwortet hat. (Genau das bietet z. B. CyberXperts.)

20 Minuten Training für die Führungskräfte – So werden sie zu Vorbildern und Multiplikatoren

Führungskräfte müssen ein Bewusstsein dafür entwickeln, dass sie eine besondere Verantwortung für das Thema Sicherheit tragen. Sie müssen den Mitarbeitern ein Vorbild sein und die Mitarbeiter immer wieder dazu ermutigen, die Sicherheitsrichtlinien einzuhalten und sich bei der täglichen Arbeit die erforderliche Sensibilität und Aufmerksamkeit für die Informationssicherheit zu bewahren.

Führungskräfte müssen geschult werden, damit sie wie jeder Mitarbeiter die Sicherheitsrichtlinien einhalten, den Mitarbeitern als Vorbild dienen, in ihrem Fachbereich Verantwortung für die Informationssicherheit übernehmen, in ihrer Personalverantwortung auch den Datenschutz ernst nehmen.

Je nach Unternehmensgröße bieten sich Präsenztrainings für Führungskräfte an oder WBT mit den genannten Inhalten. In beiden Fällen sollten die Trainings nicht länger als 20 Minuten dauern. Auch bei diesem Training ist es wichtig, auf Unterhaltung zu setzen.

Schritt 4: Messen Sie den Erfolg anhand dieser Kriterien

Erfolgsmessungen machen transparent, ob Sie mit Ihren Sensibilisierungsmaßnahmen gegen Dynamik, Beharrlichkeit und Trotz der Mitarbeiter erfolgreich waren und ob in den Trainings nachhaltig Fachwissen vermittelt wurde.

Aus den Ergebnissen können Sie direkt erkennen, an welchen Themen Sie weiterarbeiten müssen.

Spätestens jetzt wird deutlich, dass Ihre Aufgabe nicht mit der Durchführung einer Phishing-Kampagne beendet ist.

Die erste Phishing-Kampagne war der erste Schritt auf Ihrem Weg zur Etablierung einer Sicherheitskultur, auf dem Sie die gemeinsamen Ziele, Interessen, Normen, Werte und Verhaltensmuster in Ihrem Unternehmen herausbilden müssen.

Die Auswertung der Phishing-E-Mail hat Ihnen sehr genau gezeigt, wie viele Mitarbeiter anfällig für solche Angriffe sind.

Wenn Sie einen solchen Angriff ein halbes Jahr nach der ersten Kampagne wiederholen, haben Sie einen deutlichen Nachweis, ob sich die Aufmerksamkeit Ihrer Mitarbeiter verbessert hat.

Ebenso liefert Ihnen das E-Learning Informationen darüber, wie viele Mitarbeiter teilgenommen haben und wie deren Testergebnisse waren. Auch hier können Sie durch regelmäßige Auswertungen erfahren, wie der Kenntnisstand Ihrer Mitarbeiter ist.

Führen Sie weitere Prüfungen durch, mit denen Sie messbare Ergebnisse erhalten.

Erstellen Sie einen Prüfungsplan, mit dem Sie den Erfolg Ihrer Maßnahmen nachweisen können.

Mit solchen Prüfungen können Sie über einen längeren Zeitraum auswerten, ob sich das Verhalten der Mitarbeiter durch Ihre Awareness-Maßnahmen ändert.

Stellen Sie Verbesserungen fest, sollten Sie diese auch kommunizieren.

Ihrer Geschäftsleitung können Sie nachweisen, dass sich die Security-Awareness-Kampagne bezahlt gemacht hat, und die Mitarbeiter können Sie für ihre Sensibilität und ihr Fachwissen loben.

Verschlechtern sich die Ergebnisse, müssen Sie themengerecht Trainings oder Sensibilisierungsmaßnahmen durchführen. So können Sie sehr genau steuern, in welchen Themenbereichen Sie aktiv Maßnahmen ergreifen müssen.

CyberXperts Prüfung	**Methode**	**Prüfungs-gegenstand**
Phishing-E-Mail	Versand gefälschter E-Mails	Sensibilität der Mitarbeiter
E-Learning	Durchführung von digitalen Lerneinheiten	Vorhandensein von Fachwissen
Sicherheitsmeldungen	Auswertung der Help-Desk-Datenbank und Anzahl der Nachfragen zu auffälligen E-Mails	Sensibilität der Mitarbeiter
E-Mail-Verschlüsselung	Auswertung von E-Mail-Protokollen	Sensibilität der Mitarbeiter

CyberXperts macht Ihnen das Messen Ihrer Awareness-Kampagne besonders leicht:

Denn es bietet Ihnen **automatische Auswertungen Ihrer Phishing-E-Mails auf Abteilungsebene.** So sehen Sie direkt, welche Abteilung Schulungsbedarf hat und wo Sicherheitslücken entstanden sind.

Passend dazu können Sie direkt unsere E-Learning-Einheiten nutzen und die Abteilungen zu den digitalen Trainings einladen. Im Anschluss erhalten Sie einen Nachweis über die Sensibilisierungsmaßnahme für Ihre Unterlagen.

Ja, ich möchte meinen persönlichen Termin für ein Strategie-Beratungsgespräch jetzt reservieren. Hier klicken.

Mit einer Phishing-Simulation sorgen Sie für einen starken AHA-Effekt bei Ihren Mitarbeitern … und eine hohe Bereitschaft dafür, sich mit dem Thema „Cyber Security" auseinanderzusetzen.

Schritt #11: So binden Sie Lieferanten und Dienstleister in Ihr ISMS ein

Sicherheitsrisiken beim Dienstleister wirken sich auch auf Ihre interne Infrastruktur oder Ihre Lieferketten aus. Es ist daher wichtig, auf alle Risiken einzugehen, denen Ihr Unternehmen durch die Zusammenarbeit mit externen Dienstleistern ausgesetzt ist. Die Norm fordert an dieser Stelle, dass alle ausgelagerten Prozesse klar festgelegt und nachhaltig gesteuert werden. Eine wesentliche Anforderung an die Steuerung der Dienstleister ist die vertragliche Festlegung Ihrer Auditrechte beim Dienstleister. Bei der Verarbeitung personenbezogener Daten muss dies sogar gem. DSGVO vertraglich geregelt werden.

Das Verlangen nach Informationssicherheit bei Dienstleistern wird zunehmend durch Zertifizierungen beantwortet. Dafür geeignet sind ISO/IEC 27001:2013, ISO/IEC 27018 für die Verarbeitung personenbezogener Daten in einer Cloud oder – in Teilen – der internationale Standard ISAE 3402 „Assurance Reports on Controls at a Service Organization". In diesem Zusammenhang müssen Sie den Dienstleister vertraglich verpflichten, Ihnen regelmäßig unabhängige Prüfungsberichte und Zertifikate vorzulegen und Sie bei Sicherheitsvorfällen unverzüglich zu informieren.

Mein Tipp: Bei der Vorlage von ISO-27001:2013-Zertifikaten seitens der Dienstleister sollten Sie unbedingt darauf achten, dass der Scope des Zertifikats tatsächlich auch Ihre Dienstleistungen umfasst. Es kommt häufiger vor, dass z. B. Zertifikate von Rechenzentren vorgelegt werden, bei denen lediglich Teilbereiche zertifiziert wurden. Dann müssen Sie sehr genau prüfen, ob die im Rahmen der Dienstleistung genutzten Systeme auch in diesem Bereich betrieben werden.

In allen Fällen ist ein vollständiger Bericht über das Audit und seine Ergebnisse sehr wichtig, da der Scope einer Prüfung und die jeweils geprüften Kontrollen ggf. variieren können. Weiterhin sollten potenzielle Abweichungen durch den Auftraggeber gemäß eigenem Risikoappetit bewertet und ggf. in den internen Risikomanagementprozess überführt werden.

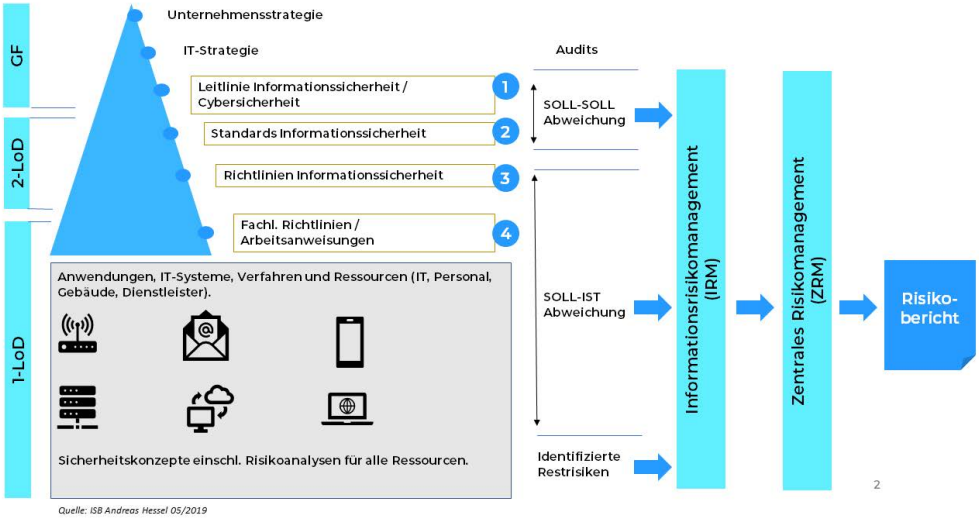
Auch im Bereich „Dienstleistersteuerung" sollten Sie Kennzahlen festlegen, um die Einhaltung Ihrer Sicherheitsziele überprüfbar zu machen. Folgende Kennzahlen haben sich in der Praxis bewährt:

- Anzahl der Dienstleisterbeziehungen, die den definierten IS-Lieferantenprozess durchlaufen haben, im Verhältnis zu allen Dienstleisterbeziehungen
- Anzahl der Dienstleister, die IS-Maßnahmen vertraglich zusichern, im Verhältnis zu allen Dienstleistern
- Anzahl der Audits bei Dienstleistern in einem Jahr im Verhältnis zu allen Dienstleistern
- Anzahl der gemessenen Richtlinienverstöße durch Lieferanten
- Anzahl der Sicherheitsvorfälle bei Dienstleistern im vergangenen Berichtszeitraum

Schritt #12: Interne Audits: So führen Sie Konformitäts-, Umsetzungs- und Wirksamkeitskontrollen durch

Die wichtigsten Ziele interner ISMS-Audits sind im Hinblick darauf zu prüfen, inwieweit das ISMS den eigenen Anforderungen des Unternehmens sowie den Anforderungen nach ISO/IEC 27001:2013 gerecht wird (Konformitätskontrolle), und die Überprüfung der Umsetzung und der Wirksamkeit der ergriffenen Maßnahmen (Umsetzungs- und Wirksamkeitskontrolle).

Dazu müssen Sie ein Auditprogramm planen und umsetzen, das Aspekte wie Häufigkeit, Verfahren, Zuständigkeiten und Verantwortlichkeiten, Planungsanforderungen, Nachverfolgung und Berichterstattung regelt. Das Auditprogramms muss optimal auf die Erreichung der IS-Ziele hinwirken und möglichst die Gesamtheit der Vorgaben aus dem ISMS abdecken. Ferner müssen Sie festlegen, wie mit Abweichungen und Schwachstellen umgegangen wird und wo diese zur weiteren Bearbeitung nachgehalten werden. Dabei können Sie sich an dem nachfolgend dargestellten Prozess orientieren.



IRM-Prozess

Schwachstellen und Abweichungen aus Audits sollten Sie in den internen Risikomanagementprozess überführen und dort mit geeigneten Maßnahmen (Risikobehandlungsplan) unterlegen.

Schritt #13: Vorfallmanagement – „Was passiert, wenn mal was passiert ...?“

Ein IT-Sicherheitsvorfall ist ein ungewolltes oder unerwartetes Ereignis oder eine Reihe entsprechender Ereignisse, die mit signifikanter Wahrscheinlichkeit die Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) bedrohen, ein hohes Schadenspotenzial haben und den Geschäftsbetrieb beeinträchtigen. Hierzu zählen beispielsweise ein Befall von IT-Systemen mit Schadsoftware, ein gezielter Cyberangriff auf die IT des Unternehmens, eine Datenpanne oder Manipulationen an Informationen und/oder IT zu Betrugszwecken. Die Bearbeitung von Sicherheitsvorfällen gehört zu den grundlegenden Aufgaben eines Informationssi-

cherheitsmanagementsystems, obwohl dies in der Norm nicht explizit aufgeführt ist.

Das Vorgehen bei einem schweren IT-Sicherheitsvorfall ist häufig vom Einzelfall abhängig. Wie lange können die Systeme offline bleiben? Wobei handelt es sich bei diesem Vorfall (Ransomware, Wirtschaftsspionage)? Ist eine Sicherung der Spuren für eine Anzeige gewünscht? Wie ist die Bedrohungslage für das Unternehmen?

Eine Umfrage bei Unternehmen zeigt sehr deutlich, dass in 30 Prozent der Fälle kein Notfallplan für Cyberangriffe vorhanden ist. Betrachtet man die Zeit, die für die Entdeckung und die Gegenmaßnahmen erforderlich ist, ist das für viele Unternehmen ein sehr hohes Risiko. Gerade in der heutigen Zeit, in der es täglich erfolgreiche Angriffe auf Unternehmen gibt, ist es umso wichtiger, Gegenmaßnahmen zu ergreifen und sich auf den Notfall vorzubereiten.

Sicherheitsvorfälle sind nicht zwingend ereignisbezogen. Auch Situationen, die bereits länger bestehen, deren Entdeckung aber den Schluss zulässt, dass ein Sicherheitsproblem für das Unternehmen besteht, werden im Rahmen der IT-Sicherheitsvorfallbehandlung behandelt.

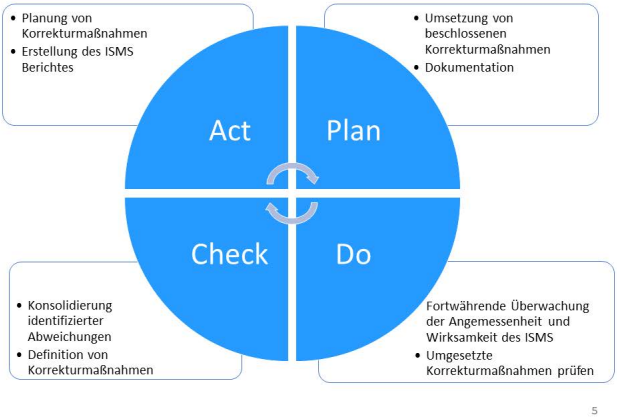
Es ist davon auszugehen, dass Ihre IT-Abteilung ggf. viele Tage lang (große) Teile ihrer Dienstleistung nicht erbringen kann oder die IT-Systeme Ihres Unternehmens nicht zur Verfügung stehen. (Erfahrungswerte bei vollständiger Kompromittierung: zwei bis vier Wochen). Im Rahmen des IT Service Continuity Managements (ITSCM) ist ein geeignetes Krisenmanagement einzurichten, das neben den technischen Wiederherstellungsaspekten insbesondere die Kommunikation mit den Stakeholdern, den Behörden und ggf. der Presse adressiert.

Sie müssen demnach in Ihrem Unternehmen Prozesse und Verantwortliche festlegen, die sicherstellen, dass im „Ernstfall“ sachgerecht gehandelt wird. Dazu benötigen Sie regelmäßig die nachfolgenden Dokumente:

- Incident-Response- oder Notfallplan, inklusive aktueller Kontaktlisten und Eskalationspläne
- Verhaltensregeln bei sicherheitsrelevanten Ereignissen oder Sicherheitsvorfällen
- Prozessbeschreibungen und Arbeitsanweisungen für die Sicherung von Beweisen (Forensik)
- Dokumentation und Berichte zu den einzelnen Vorfällen

Schritt #14: Kontinuierlicher Verbesserungsprozess, bei dem ALLE im Unternehmen mithelfen

Wenn Sie in Ihrem Unternehmen ein normkonformes ISMS betreiben möchten, müssen Sie organisatorische Maßnahmen festlegen, auf deren Basis eine kontinuierliche Verbesserung gezielt und planmäßig stattfindet. Die Durchführung dieser Maßnahmen und die jeweiligen Ergebnisse sind hierbei zu überwachen und angemessen zu dokumentieren. Darüber hinaus müssen Sie nachweisen, wie sie bei festgestellten Mängeln dafür sorgen, dass sich diese nicht wiederholen. Hierfür eignet sich der in vielen Managementsystemen genutzte Plan-Do-Check-Act- (PDCA) Zyklus.



PDCA-Zyklus im ISMS

Gemäß ISO 27001:2013 sind bei Auftreten bzw. Erkennung von Abweichungen (Nichtkonformität) Maßnahmen zur Überwachung und Korrektur zu ergreifen und die Wirksamkeit dieser zu überprüfen. Die Notwendigkeit und Dringlichkeit der Beseitigung von Abweichungsursachen ist nach folgendem Muster zu bewerten:

- Analyse der Abweichung und der zu erwartenden bzw. bereits bestehenden Auswirkungen
- Feststellung der Abweichungsursache(n)
- Überprüfung, ob vergleichbare Abweichungen bestehen oder möglicherweise auftreten könnten

Für das Erkennen von potenziellen oder bereits bestehenden Abweichungen und deren Ursachen sowie für die Definition von entsprechenden Korrekturmaßnahmen ist regelmäßig der ISB verantwortlich. Korrekturmaßnahmen müssen den Auswirkungen der aufgetretenen oder erkannten Abweichung angemessen sein. Sie müssen dabei dokumentieren, welcher Art eine aufgetretene Abweichung ist, welche Maßnahmen zur Überwachung und Korrektur beschlossen und welche Ergebnisse durch die Umsetzung erreicht wurden.

Die Umsetzung von definierten Korrekturmaßnahmen wird vom ISB initiiert und in Abstimmung mit den jeweiligen Verantwortlichen bzw. Asset-Eigentümern umgesetzt. Parallel müssen Sie als ISB prüfen, ob durch die Korrekturmaßnahme eine Änderung der ISMS-Dokumentation und der Prozesse notwendig wird. Die Ergebnisse der Umsetzung müssen Sie dokumentieren. Zudem sollten Sie die Ergebnisse in Ihren ISM-Bericht aufnehmen.

Der Wald vor lauter Bäumen … Wie Sie Ihr ISMS Schritt für Schritt aufbauen

Eine Zertifizierung nach ISO 27001:2013 muss nicht immer Ihr gesamtes Unternehmen umfassen. Sie können sich zunächst auf die wesentlichsten IT-Systeme und Verfahren (IT-Verbund) beschränken. So können Sie z. B. zunächst Ihr Kundenportal, Ihr Warenwirtschaftssystem oder Ihr Rechenzentrum zertifizieren lassen. Damit können Sie die Komplexität und den Aufwand erheblich reduzieren.

Die größte Herausforderung bei einer Zertifizierung liegt darin, dass ein ISMS nach ISO 27001:2013 tatsächlich einen Kulturwandel in Ihrem Unternehmen auslösen muss und auch auslösen wird. Diesen Change-Prozess so zu begleiten, dass Ihre Stakeholder und auch Ihre Mitarbeiter nicht „auf der Strecke" bleiben, erfordert ein hohes Maß an Fachkompetenz und vor allem Sozialkompetenz. Daher sollten Sie sich nicht zu viel auf einmal vornehmen. Lassen Sie sich und Ihrem Unternehmen die Zeit, die

Sie benötigen, um diesen Change-Prozess gemeinsam zu durchlaufen. Sonst verlieren Sie die Unterstützung aller Beteiligten und haben keine Möglichkeit, ein sachgerechtes ISMS aufzubauen.

Der große Wurf oder besser das Wichtigste zuerst

Sie können anstelle der ISO 27001:2103 für einzelne IT-Verbünde auch eine Zertifizierung nach BSI-Grundschutz durchführen. Dabei gibt es eine „IT-Grundschutz-Einstiegsstufe“ und eine „Aufbaustufe“. Diese unterscheiden sich im Wesentlichen in Hinsicht auf den Umfang und die Komplexität der Anforderungen. Damit können Sie sich schrittweise an eine Zertifizierung nach ISO 27001:2013 herantasten. Je nach Sicherheitsanspruch, den Ihr Unternehmen hat, ist vielleicht eine Zertifizierung nach der „IT-Grundschutz-Einstiegsstufe“ sinnvoll und ausreichend. Sprechen Sie mit Ihrer IT-Abteilung und prüfen Sie gemeinsam, welcher Weg für Ihr Unternehmen der beste ist.

CyberXperts – die geniale neue Lösung für Ihre nächste Awareness-Kampagne

Modul 1: Mit diesen stets aktuellen Schulungsvorlagen sensibilisieren Sie Ihre Mitarbeiter wirksam für Cyber-Fallen!

Ihre Mitarbeiter sind Ihre Human Firewall und schützen Ihr Unternehmen. Schulungslücken und fehlende Awareness sind das größte Risiko für Sie. Zeitdruck und Unvorsichtigkeit im Berufsalltag sind das Einfallstor für Angreifer.

Sicher ist Ihr Unternehmen nur, wenn Awareness zur Routine wird.

Mit dem starkem Bild- und Videomaterial von CyberXperts sensibilisieren Sie Ihre Mitarbeiter wirksam und langanhaltend.

Stets aktuelle Schulungen sorgen dafür, dass Ihre Mitarbeiter bei den ständig neuen Bedrohungen immer auf dem neuesten Stand sind.

Dabei gehen wir bei CyberXperts nach diesen Prinzipien vor:

- **Positives Reinforcement:** Kontinuierliche Schulungs-Einheiten sorgen für einen nachhaltigen Lern-Effekt
- **Kein trockenes E-Learning, kein Frust:** Gamifizierung und Interaktion bringen Interesse und Motivation.
- **Echte Beispiele aus der Realität:** Reale Situationen unterstreichen die Relevanz des Themas und zeigen, wie raffiniert Cyberkriminelle vorgehen!
- **Maßgeschneidert für Ihr Unternehmen** Unser E-Learning können Sie mit Ihrem Unternehmenslogo individualisieren und an Ihre Corporate Identity anpassen.

Modul 2: Die perfekte Phishing-Simulation: So identifizieren Sie Schulungs-Potenzial und erhalten einen Nachweis für die ISO 27001

Mit simulierten Phishing-E-Mails lernen Ihre Mitarbeiter effektiv Angriffe zu erkennen und im Ernstfall richtig zu reagieren. Die automatisierten Phishing-Kampagnen von CyberXperts können Sie individuell an Ihr Unternehmen anpassen und aussteuern.

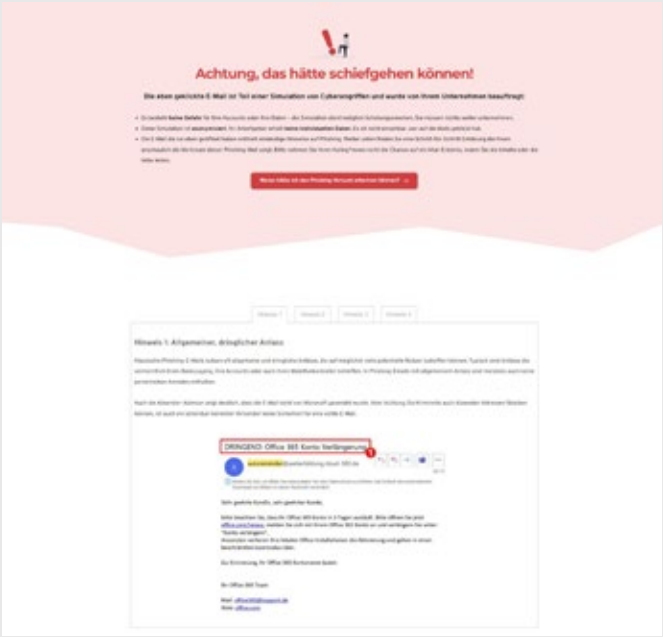
Ihre Auswertung zeigt Ihnen das Schulungspotential und kann als **Nachweis für Cyber-Versicherungen und die ISO 27001** genutzt werden.

So geht's:

Wir besprechen in einem persönlichen Gespräch mit Ihnen wie Ihre persönliche Kampagne aufgesetzt werden soll: Sie wählen, ob alle oder nur einzelne Abteilungen E-Mails erhalten und in welchem Abstand. Für eine möglichst realistische Simulation berücksichtigen wir, welche Tools und Software in Ihrem Unternehmen standardmäßig verwendet werden.

1. **Let's phish! Die Test-E-Mails gehen raus.** Nachdem Ihre Kampagne eingerichtet wurde, versenden Sie eine unangekündigte Test-Phishing-E-Mail, die Sie zum Startschuss Ihrer Kampagne machen. Danach werden in regelmäßigen Abständen simulierte Phishing-E-Mails automatisiert an Ihre Mitarbeiter versendet. Sie brauchen sich um nichts mehr zu kümmern. Falls ein Mitarbeiter klickt, erhält er einen Hinweis und kann direkt lernen, wie er eine solche Panne beim nächsten Mal vermeiden kann.
2. **Eine automatische Auswertung Ihrer Phishing-Kampagne wird für Sie generiert.** Hier erfahren Sie, wie viel Prozent Ihrer Mitarbeiter geklickt haben und in welchen Abteilungen Schulungsbedarf besteht.

Jetzt gratis Phishing-Simulation für Ihr Unternehmen durchführen: Reservieren Sie einfach hier Ihr persönliches Strategie-Gespräch!



Mit einer Phishing-Simulation sorgen Sie für einen starken Aha-Effekt bei Ihren Mitarbeitern … und einer hohen Bereitschaft dafür, sich mit dem Thema CyberSecurity auseinanderzusetzen.

Modul 3: Mit einem intuitivem 360°-Check zur Einschätzung Ihres Risikoprofils kennen Sie die Sicherheitslage Ihres Unternehmens genau

CyberXperts hilft Ihnen dabei, aktuelle Gefahren zu identifizieren und geeignete Gegenmaßnahmen umzusetzen. So haben Angreifer bei Ihrem Unternehmen keine Chance!

Mit dem CyberXperts-Dashboard sehen Sie alle Risiken auf einem Blick. Mit ausgewählten Fragen analysieren wir Ihr Risikoprofil und zeigen mögliche Szenarien.

Verständliche Schritt-für-Schritt-Maßnahmen

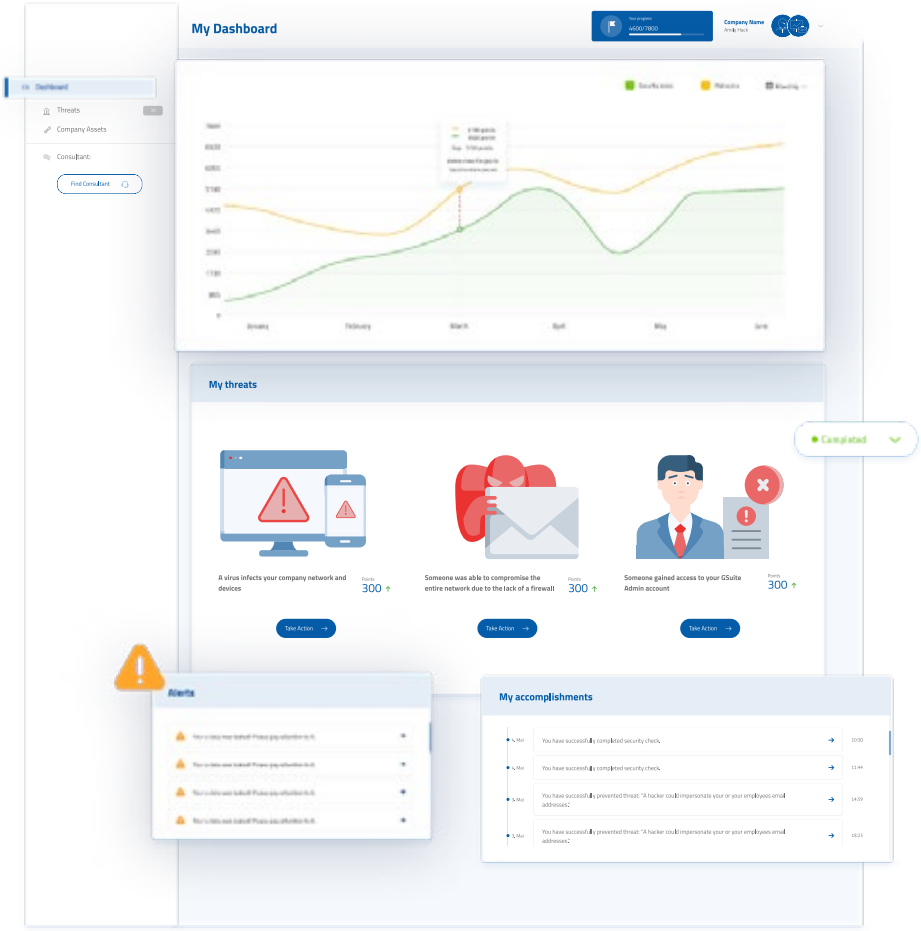
Sie erhalten zu jeder potenziellen Bedrohung individuelle Maßnahmen, um Ihr Unternehmen besser zu schützen. Mit einer leicht verständlichen Schritt-für-Schritt-Anleitung können Sie diese kinderleicht in Ihrem Unternehmen umsetzen.

Immer im Blick und automatische Erinnerungen

Damit Ihre IT-Sicherheit im Alltagsstress nicht in Vergessenheit gerät, erinnern wir Sie rechtzeitig daran und analysieren die aktuelle Sicherheitslage Ihres Unternehmens.

Ja, ich möchte mehr über den 360°-Check für mein Unternehmen erfahren.

Wir freuen schon auf Ihre Terminvereinbarung!


My Dashboard
Company Name
Threats
Company Assets
Consultant
Find Consultant
My threats
Completed
A virus infects your company network and devices
Points
300
Take Action
Someone was able to compromise the entire network due to the lack of a firewall
Points
300
Take Action
Someone gained access to your GSuite Admin account
Points
300
Take Action
Alerts
My accomplishments
You have successfully completed security check.
You have successfully completed security check.
You have successfully prevented threat: "A hacker could impersonate your or your employees email addresses."
You have successfully prevented threat: "A hacker could impersonate your or your employees email addresses."

Impressum

CyberXperts

ein Unternehmensbereich der
VNR Verlag für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2-4; D-53095 Bonn

Vorstand: Richard Rentrop

Telefon: 0228 - 9 55 01 60 (Kundendienst)
Telefax: 0228 - 3 69 64 80
E-Mail: info@cyberxperts.de
Internet: https://www.cyberxperts.de

Verantwortlicher i.S.d.P.: Michael Jodda, Theodor-Heuss-Straße 2–4, 53177 Bonn

Enthält u. a. Artikel von Andreas Hessel

Satz: BB-Design, Birken-Honigsessen

Bildnachweis: S. 1 Looker_Studio, S. 14 H_Ko, S. 16 The Cheroke, S. 18 NDABCREATIVITY, S. 26 amedeoemaja, S. 31 ASDF, S. 33 FarknotArchitect, S. 35 Editable Line icons, S. 37 davooda, S. 38 fizkes, S. 39 fizkes, S. 40 MacroOne Phishing, S. 43 blankstock, S. 45 fizkes, S. 50 Jirapong, S. 53 NicoLeNino, S. 57 freebird7977 – alle AdobeStock;
Infografiken – A. Hessel und CyberXperts;

Bonn, Berlin, Bukarest, Jacksonville, Manchester, Warschau