Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

Schutzschild Mensch - 10 Goldene Regeln

ANDREAS NEUENFELS

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Impressum

HERAUSGEBER
Mittelstand-Digital Zentrum Chemnitz
Tel: 0371 531 19935
Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

REDAKTION Anikó Lessi

GESTALTUNG
PUNKT191 – Marketing und Design
www.punkt191.de

BILDNACHWEIS TITEL
Mike.shots - Freepik.com

VERÖFFENTLICHUNG August 2022

Schutzschild Mensch - 10 goldene Regeln

Auf der Basis jahrelanger Erfahrungen und in enger Zusammenarbeit mit Unternehmen geben wir zehn goldene Regeln weiter, wie Sie für Ihre IT-Sicherheit einen „Schutzschild Mensch“ aufbauen können. Die Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen sowie dem Handwerk.

Erfahren Sie in diesem Nachgelesen:

- Warum stellt der Mensch ein wichtiges Glied der IT-Sicherheit dar?
- Wieso kann der Mensch auch ein Unsicherheitsfaktor sein?
- Welche Aspekte müssen für den Menschen im Rahmen der IT-Sicherheit betrachtet werden?
- Wie kann der Schutzschild Mensch aufgebaut werden?
- Was sind technische Unterstützungsmöglichkeiten für Menschen?
- Wie können richtige Verhaltensweisen vorgegeben werden?
- Wie kann der Schutzschild Mensch ein nachhaltig hohes IT-Sciherheitsniveau erreichen?

Warum ist der Schutzschild Mensch so wichtig?

Der Mensch ist ein wichtiger Bestandteil von unternehmerischen Arbeitsprozessen. Hieraus folgt die Notwendigkeit, dass dieser mit Informationen und Daten umgeht oder Informations- und Kommunikationstechnologien (IKT) nutzt. Diese haben die Arbeit in den letzten Jahrzehnten wesentlich verändert und in vielen Bereichen effizienter gemacht – was auch in der Natur des Menschen liegt. Sie sind stets bemüht, Arbeitsvorgänge einfacher zu gestalten.

Gleichzeitig ist der Mensch ein soziales Wesen und gibt Informationen bewusst oder unbewusst an andere Menschen weiter.

Warum können Menschen ein Unsicherheitsfaktor sein?

Generell entstehen im Umgang mit IKT-Geräten und Informationen bzw. Daten Gefahren wie z. B. Fehlkonfigurationen, unbeabsichtigtes Löschen von Dateien oder die Nutzung unsicherer mobiler Endgeräte bzw. Speichermedien. Viele Unsicherheiten sind dabei dem menschlichen Verhalten geschuldet, da versucht wird, möglichst einfache Prozesse durchzuführen („Workarounds“ von Sicherheitsmaß-

nahmen, Nutzung von unsicheren Passwörtern) oder sensible Daten weitergegeben werden. Letzteres kann sowohl wissentlich als auch unwissentlich geschehen. Häufig verfügen Personen im Umgang mit Informationen und technischen Geräten nicht über das notwendige Wissen zu Gefahrenquellen oder sind nicht genügend über mögliche Angriffsversuche durch Dritte (z. B. Phishing, Social Engineering) aufgeklärt. Eine bewusste Weitergabe von Daten kann ebenfalls durch Dritte initiiert werden (z. B. CEO-Fraud) oder aber aufgrund eigener Motivation (z. B. Sabotage).

EXKURS SOCIAL ENGINEERING

Das Social Engineering (im Unternehmenskontext) ist ein Angriffsvektor, bei dem Dritte durch Anwendung verschiedener Methoden, das Handeln von Mitarbeitenden manipulieren, um an Informationen zu gelangen oder Zugriff zu IT-Systemen zu erhalten.[1] Hierbei werden vor allem menschliche Eigenschaften (z. B. Hilfsbereitschaft, Vertrauen oder Angst) ausgenutzt oder über Täuschungen realisiert. Klassische Methoden des Social Engineerings sind (Spear-)Phishing, Baiting oder Media Dropping.[2]

Wie lässt sich der Schutzschild Mensch aufbauen?

Ein funktionierender „Schutzschild Mensch“ ist dann aufgebaut, wenn er Gefahren erkennen und durch sein Verhalten kein Schaden entstehen kann. Dies ist in der Praxis nur anwendbar, wenn beim Anlass (also die eigentliche Gefahr) Motivation und Wissen zur IT-Sicherheit beim Mitarbeitenden vorhanden sind. Diese können im Wesentlichen durch folgende Aspekte realisiert werden:

- Sensibilisierung und Bewusstsein,
- Richtlinien und Regeln im Umgang mit IKT und Daten sowie
- technischen Unterstützungsmaßnahmen.

Wie kann ein Bewusstsein zur IT-Sicherheit geschaffen werden?

Regel 1: Mitarbeitende informieren

Machen Sie Ihre Mitarbeitenden ständig auf aktuelle Gefahrenlagen aufmerksamen. Nutzen Sie hierfür regelmäßig Informationsmöglichkeiten in Dienstberatungen, Newslettern oder Intranetbeiträgen. Auch interne Gespräche und Workshops sind eine gute Gelegenheit Themen zum Datenschutz und der IT-Sicherheit anzubringen. Zusätzlich können Sie auf kostenlose Sensibilisierungsformate von Mittelstand-Digital und weiteren Projekten[3] oder unterschiedliche Lösungen am Markt zurückgreifen.

Regel 2: Personal weiterbilden

Aufbauend auf Regel 1 sollten Sie möglichst viel Mitarbeitende zum Thema IT-Sicherheit weiterbilden. Neben den klassischen IT-Verantwortlichen, umfasst dies insbesondere Stellen, bei denen viel mit personenbezogenen, wirtschaftlichen oder unternehmenswichtigen Daten gearbeitet wird. Hierbei sollten Sie auch die Anforderungen der Datenschutzgrundverordnung beachten.

Regel 3: Bewusstsein und Wissen prüfen

Sie sollten in regelmäßigen Abständen prüfen, ob Ihre Weiterbildungs- und Sensibilisierungsmaßnahmen auch tatsächlich erfolgreich waren. Hierbei könnten Sie z. B. auch Rückschlüsse aus Workshops gewinnen oder auf gamifizierte Anwendungen zurückgreifen. Letztere können u. a. Phishing per Mails simulieren und das Nutzerverhalten auswerten. [4,5]

Wie können Verhaltensweisen vorgegeben werden?

Regel 4: Verantwortlichkeiten festlegen

Legen Sie Personen fest, welche über ein hohes IT-Sicherheitsbewusstsein verfügen und anderen Mitarbeitenden als Ansprechpartner bei Fragen (z. B. ob es sich um eine betrügerische Webseite oder E-Mail handeln könnte) zur Verfügung stehen. Darüber hinaus sollten Verantwortlichkeiten so festgelegt werden, dass auch eine Problembehandlung (bei Störungen oder Notfällen) initiiert werden kann.

Insofern Ihnen keine Mitarbeitenden zur Verfügung stehen, könnten auch Externe bzw. der IT-Dienstleister mögliche Kontaktpersonen sein.

Regel 5: Richtlinien, Regeln und Prozesse zur IT-Sicherheit aufbauen

In Ihrem Unternehmen sollten Sie grundlegende Regeln und Richtlinien zur IT-Sicherheit festlegen (verschriftlichen), schrittweise Ausbauen sowie Prozesse beschreiben. Hierbei können Sie sich an einem Informationssicherheitsmanagementsystem (z. B. BSI Grundschutz[6] oder VDS 10000[7]) orientieren. Grundlegende Themen sollten dabei Regeln zur Datensicherung, dem Umgang mit mobilen End- und Speichergeräten, der Nutzung von Passwörtern in firmenrelevanten Accounts sowie dem Verhalten mit Internet und E-Mail umfassen.

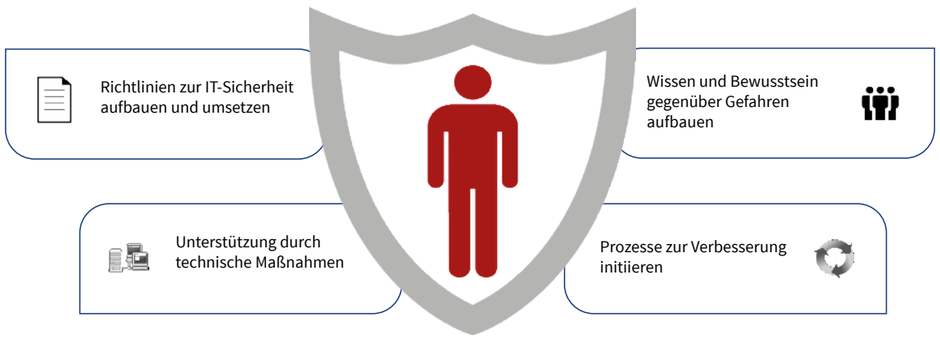
Regel 6: Reaktion auf Sicherheitsvorfälle definieren

In Ergänzung zu Regel 5 sollten insbesondere Richtlinien und Abläufe für evtl. Schadens- bzw. Sicherheitsvorfälle definiert werden. Je nach Schweregrad sollten entsprechende Handlungsweisen für die Mitarbeitenden vordefiniert sein. Eine so genannte „Notfallkarte“ oder ein „Notfallplan“ kann entsprechend unterstützend wirken. Weitere Informationen erhalten Sie im Nachgelesen: „Was tun bei einem Sicherheitsvorfall?“.

Welche technischen Maßnahmen unterstützen den Schutzschild Mensch?

Regel 7: Technologien zur Minimierung von Fehlverhalten einführen

Die IT-Infrastruktur im Unternehmen ist so zu gestalten, dass Fehlverhalten vermieden werden kann. Neben dem üblichen Sperren von Ports oder Schnittstellen, können intelligente Web- und Mail-Proxys ein sichereres Arbeiten im Internet ermöglichen. Diese Systeme können z. B. durch Malware- oder Schlagwortscans auf gefährliche Inhalte aufmerksam machen, wodurch Mitarbeitende noch besser sensibilisiert werden.



Elemente zum Aufbau des „Schutzschild Mensch“

Regel 8: Maßnahmen zur Unterstützung von gutem Verhalten initiieren

Mitarbeitende können auch selbstständig zur IT-Sicherheit beitragen. Dieses Verhalten sollte unterstützt werden. Möglichkeiten dafür sind z. B. die Einbeziehung bei der Bewertung von Spam-Mails und entsprechendes, automatisiertes Feedback oder eine visuelle, positive Unterstützung bei der Wahl von sicheren Kennwörtern. Honorierung und Anerkennung durch Vorgesetzte, z. B. bei der Erkennung von Sicherheitslücken oder Sicherheitsvorfällen sollten ebenfalls selbstverständlich sein.

Regel 9: Systeme zur Erkennung von Unregelmäßigkeiten einbinden

Zur Erweiterung der menschlichen Einschätzung von Gefahrenlagen können auch erweitere technische Systeme (z. B. Intrusion Detection Systeme[8]) durch Lösungen zur Anomalieerkennung und dem Monitoring unterstützen. So können mögliche Gefahrenlagen automatisch erkannt und anschließend durch Mitarbeitende bestätigt werden.

Weiterhin existieren auch Systeme, die Kontaktinformationen auf Plausibilität prüfen können. Hierdurch kann die Vertraulichkeit und Authentizität von Informationen unterstützt werden.

Wie kann der Schutzschild Mensch nachhaltig ein hohes IT-Sicherheitsniveau erreichen?

Regel 10: Prozesse zur Verbesserung initiieren

Sorgen Sie dafür, dass die IT-Sicherheit von der gesamten Belegschaft gelebt wird. Holen Sie sich dabei auch Meinungen und Verbesserungsvorschläge zu bestehenden Regeln und Prozessen von den Mitarbeitenden ein. Sollten Prozesse fehlerhaft oder nur durch Workarounds praktikabel sein, so tragen diese nicht ausreichend zu Ihren Schutzzielen bei. Deshalb sind die festgelegten Maßnahmen regelmäßig mit dem Personal auf den Prüfstand zu stellen und kontinuierlich zu verbessern.

Anmerkungen/Quellen

1. Social Engineering – der Mensch als Schwachstelle. Bundesamt für Sicherheit in der Informationstechnik. Abgerufen 10. August 2022, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html
2. Laufenburg, R. (2019, März 29). Social Engineering. It-service.netWORK Blog. https://it-service.network/blog/2019/03/29/social-engineering-methoden/
3. IT-Sicherheit in der Wirtschaft. Bakgame.de. Abgerufen 9. August 2022, https://www.bakgame.de/
4. SoSafe Security. Phish-Test - Kostenlose Phishing-Simulation für Bürgerinnen und Bürger. Phish-Test. Abgerufen 10. August 2022, https://www.phish-test.de/
5. KnowBe4 Germany Security Awareness Training. Knowbe4.de. Abgerufen 10. August 2022, https://www.knowbe4.de/
6. IT-Grundschutz Informationssicherheit mit System. Bund.de. Abgerufen 12. August 2022, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
7. VdS 10000 - Informations-Sicherheit für KMU. Vds.de. Abgerufen 12. August 2022, https://vds.de/kompetenzen/cyber-security/vds-richtlinien/anforderungsrichtlinien-/-leitfaeden/vds-10000-informations-sicherheit-fuer-kmu
8. BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen. Bund.de. Abgerufen 11. August 2022, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/IDS02/index_htm.html

Autor

ANDREAS NEUENFELS ist Projektmanager bei der tti Technologietransfer und Innovationsförderung Magdeburg GmbH. Im Mittelstand-Digital Zentrum Chemnitz ist er als Mitarbeiter im Bereich IT-Sicherheit tätig.
andreas.neuenfels@digitalzentrum-chemnitz.de

Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

WAS IST MITTELSTAND-DIGITAL?
Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren, der Initiative IT-Sicherheit in der Wirtschaft und Digital Jetzt umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Platz für Ihre Notizen

Mittelstand-Digital
Zentrum
Chemnitz

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages