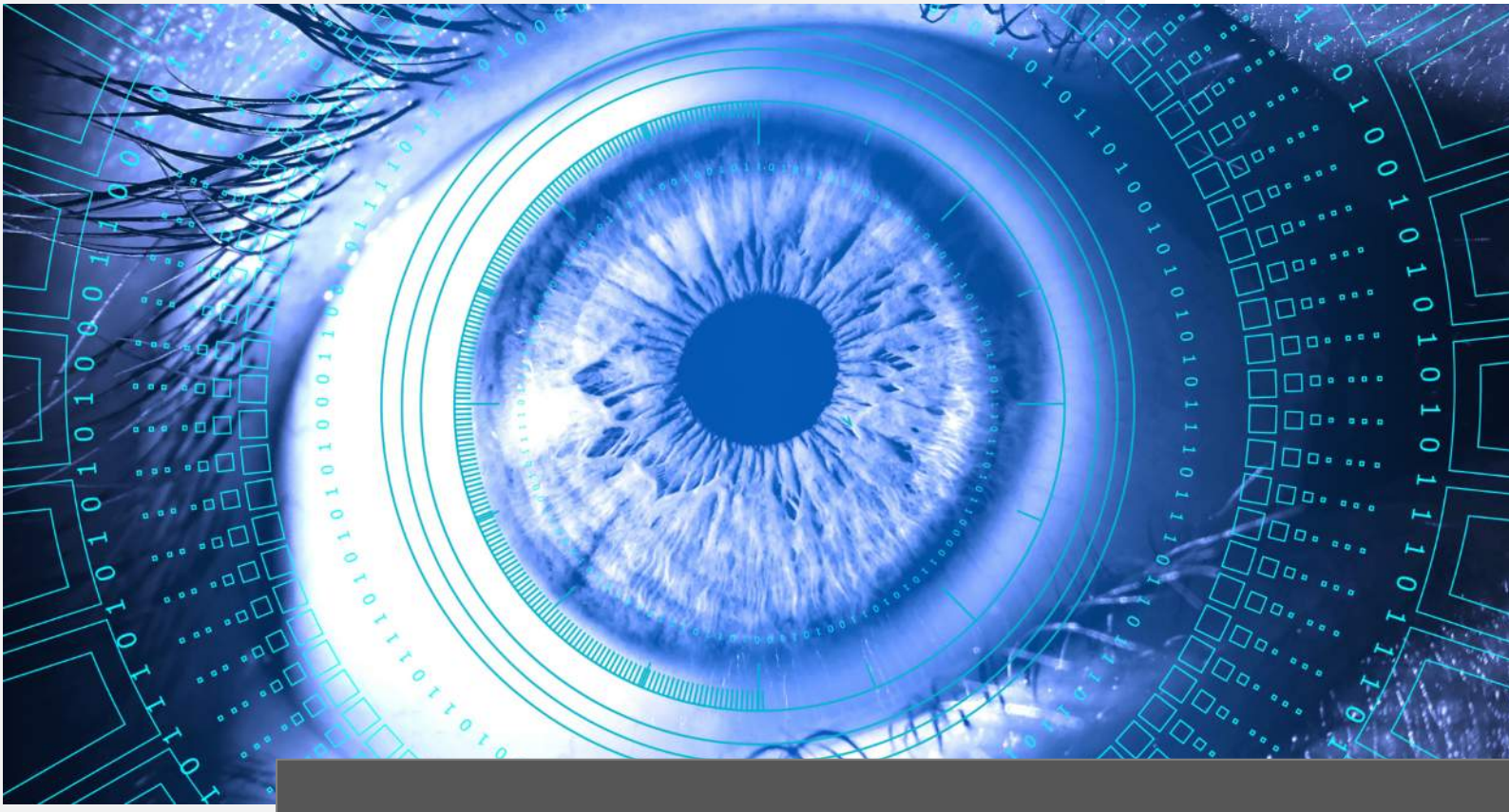
Mitarbeiter-Awareness

Aktivieren Sie die menschliche Firewall

Oktober | 2022



Wichtige Datenschutzinformationen für Ihr Unternehmen

CompuSaar

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Alexander Eich

Liebe Leserin, lieber Leser,

seit Jahren sind Unternehmen jeglicher Größe und Branche von Computerkriminalität betroffen – Tendenz stark steigend. Dabei sind die Methoden, um IT-Systeme anzugreifen, nicht nur vielfältiger, komplexer und ausgeklügelter geworden, sondern richten sich auch immer öfter gegen das Personal, welches die Attacken, ohne entsprechende Sensibilisierung, kaum noch identifizieren kann - ein hohes Risiko für jedes Unternehmen.

Ist ein Unternehmen erst einmal von einem Angriff betroffen, ist in den meisten Fällen auch der Datenschutz involviert, da Cyberangriffe meldepflichtige Vorfälle nach sich ziehen, sowohl bei den Aufsichtsbehörden als auch bei den Betroffenen. Zudem wird, neben enormer finanzieller Schäden, auch schnell das Image des Unternehmens in Mitleidenschaft gezogen.

Somit sollte sich jedes Unternehmen, zusätzlich zu den technisch möglichen Sicherheitsmaßnahmen, auch immer mit dem Thema „Awareness“ auseinandersetzen, sprich mit der Sensibilisierung aller Mitarbeiter:innen des Unternehmens.

Nur was bedeutet „Mitarbeiter-Awareness“? Wie könnte eine erfolgreiche Awareness-Strategie aussehen und wie aktiviert man eine menschliche Firewall?

Um Sie genau bei diesen Fragen zu unterstützen, haben wir uns in dieser Datenschutzzeitung ausführlich diesem Thema angenommen und Ihnen die wichtigsten Punkte zusammengetragen.

Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung zum Thema Datenschutz im Allgemeinen wünschen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung.

Sie erreichen uns unter der Telefonnummer 06894-387970 oder per E-Mail an datenschutz@compusaar.de.

Mit besten Grüßen

Alexander Eich

Faktor Mensch in der IT-Sicherheit

Wer IT-Sicherheit hört, denkt immer zuerst an technische Maßnahmen, wie Firewall, Antivirensoftware oder ein Mobile Device Management. Der Faktor Mensch wird in diesen Konzepten häufig nicht oder nur wenig berücksichtigt, wodurch genau diese „Schwachstelle“ immer mehr in den Fokus der Angreifer rückt – man nennt dies *Social-Engineering*.

Hinzu kommt eine immer schwieriger werdende Dezentralisierung der Angestellten. Zum Schutze der Gesundheit arbeiten aktuell viele Mitarbeiter:innen vermehrt von zu Hause oder anderen Remotestandorten aus und der Trend zeigt, dass auch zukünftig das Homeoffice eher die Regel als eine Ausnahme darstellen wird.

Durch diese Arbeitsweise werden die Angestellten unabsichtlich voneinander „getrennt“ und der direkte Austausch am Kaffeeautomaten oder in der Kantine entfällt. Dadurch werden sicherheitsrelevante Informationen nur verzögert oder teilweise gar nicht ausgetauscht und eine zeitnahe und ggf. dringliche Kommunikation bei einem Zwischenfall kann so zu einer enormen Herausforderung für jedes betroffene Unternehmen werden.

Cyberkriminelle haben hierzu eine Vielzahl von Angriffsmethoden entwickelt, die technischen Barrieren zu umgehen, indem sie gezielt Personen mit falschen E-Mails, Anrufen, uvm. „angreifen“ und vor Herausforderungen stellen, die eigenständig und teilweise emotional gemeistert werden müssen. Für viele – ohne eine gute Vorbereitung auf diese Gefahren – eine zu hohe Verantwortung.

Genau diese Social-Engineering-Angriffe gewinnen aber immer mehr an Bedeutung, was sich in einer Studie der ENISA[1] (Agentur der Europäischen Union für Cybersicherheit) wiederspiegelt. Hier wurde im Zusammenhang mit der Corona-Pandemie ein Anstieg um 600% von Phishing-Mails und -Webseiten festgestellt. Auch andere geopolitische Krisen werden genutzt, um Unternehmen zu schaden. Selbst vor Bertreibern kritischer Infrastrukturen (wie z.B. Krankenhäusern) schrecken die Angreifer mittlerweile nicht mehr zurück!

Um die stark zunehmenden Cybergefahren zu minimieren, sollten alle Personen im Unternehmen mit den Methoden der Angreifer vertraut gemacht werden, so dass Angriffe frühzeitig erkannt und im Sinne der IT-Sicherheit, des Datenschutzes und aller sensiblen Unternehmensdaten gehandelt werden kann.

Diese Mitarbeitersensibilisierung nennt man auch Mitarbeiter-Awareness - ein entscheidender Baustein auf dem Weg zur ganzheitlichen IT- und Datensicherheit.

during-the-covid-19-pandemic

Was wird unter einem Awareness-Konzept verstanden?

Awareness | Definition

Im Zusammenhang mit den Gefahren für die IT-Umgebung einer Organisation spricht man von der „**Security-Awareness**“. Hierbei wird das „Sicherheits-bewusstsein“ der Mitarbeiter:innen geschärft, indem sie zu Themen wie IT-Sicherheit, Cybersecurity und Datenschutz sensibilisiert werden. Es wird auf bestehende Gefahren hingewiesen und deutlich gemacht, welche Risiken existieren und worauf Cyberkriminelle abzielen. Dadurch soll ein Fehlverhalten des Personals verhindert und ggf. Angriffe auf die Unternehmensinfrastruktur selbständig erkannt, verhindert und gemeldet werden.

Gem. Datenschutzgrundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG) muss der Verantwortliche seiner Einhaltung der Rechenschaftspflicht nachkommen. Dieses beschreibt zwar keine Verpflichtung zur Unterweisung von Mitarbeiter:innen, doch sind je nach Aufgabengebiet entsprechende technische und organisatorische Maßnahmen umzusetzen, um die personenbezogenen Daten zu schützen.

Awareness vs. Schulung?

Im Gegensatz zu einer Mitarbeiterschulung geht die Awareness einen Schritt weiter. Neben der Vermittlung von themenorientierten Inhalten („Kennen und Erkennen“) werden anhand praktischer Beispiele der direkte Bezug zur Praxis hergestellt („Anwenden“) und schließlich die Mitarbeiter:innen regelmäßig in der Praxis getestet („Abwehren und Verbessern“), z.B. durch Phishing-Simulationen.

Awareness-Konzept

Das Awareness-Konzept ist nun die strategische Umsetzung der Sensibilisierung. Hierdurch soll eine zielgerichtete Entwicklung des Sicherheitsbewusstseins im Unternehmen gewährleistet werden. Die Awareness-Kampagnen werden in die Unternehmensprozesse integriert und sorgen zum einen für praktischen Bezug bei der täglichen Arbeit (Berücksichtigung spezifischer Bedürfnisse), zum anderen, dass bestehende Richtlinien eingehalten werden.

Die folgenden Seiten sollen exemplarisch zeigen, wie Unternehmen in 6 Schritten eine vereinfachte Awareness-Kampagne implementieren können.

Aufbau einer IT-Security-Awareness-Kampagne

01 Security-Awareness ist Chefsache!

Sowohl der BSI-Grundschutz als auch andere Normen mit Bezug zur IT-Sicherheit (ISO 27001, VdS 10000, etc.) verweisen in Ihren Dokumentationen auf die *„Sensibilisierung und Schulung zur Informationssicherheit“*.

Idealerweise sollte die Motivation des Managements jedoch nicht darin liegen *„Normen zu erfüllen“*, sondern selbst eine Vorbildfunktion auszuüben. Sie sollten Mitarbeiter:innen dazu bringen, aktiv zum Schutz des Unternehmens beizutragen.

Zudem müssen genügend Ressourcen geschaffen und Verantwortlichkeiten definiert werden. Je nach Unternehmensbranche können hier verschiedene Zielgruppen Bestandteil der Kampagne sein:

- Informationssicherheitsbeauftragter
- Datenschutzbeauftragter
- IT-Leitung
- Ggf. Betriebsrat
- Weitere branchenspezifische Stakeholder

02 Bekanntmachung einer Awareness-Kampagne

Mit dem Start einer neuen Awareness-Kampagne, sollte das Personal direkt in die Maßnahme integriert und der Sinn und Zweck verdeutlicht werden. Schließlich geht es um die Sicherheit der Unternehmensdaten, den eigenen personenbezogenen Daten, um das Unternehmen selbst und somit schlussendlich um den eigenen Arbeitsplatz.

In der Praxis haben sich hierfür die Bekanntgabe durch einen Informationssicherheitsbeauftragten, eine Info-Veranstaltung im Rahmen einer Betriebsveranstaltung oder Info-E-Mails mit tatsächlichen Vorfällen bewährt (z.B. *„Cyber-Angriff auf fünf Rundfunkanstalten“*, *„Ransomware-Attacke auf Garmin“* oder *„Cyberangriff auf Media Markt & Saturn“*).

Weitere Maßnahmen, um die Themen einer Awareness-Kampagne aufzugreifen, könnten Intranet-News oder Merkblätter für alle Mitarbeiter:innen sein. Auch individuell mit Sicherheitsinformationen gestaltete Medien (z.B. Tassen, Mauspads, …) können bei der Verteilung der Informationen sehr hilfreich sein.

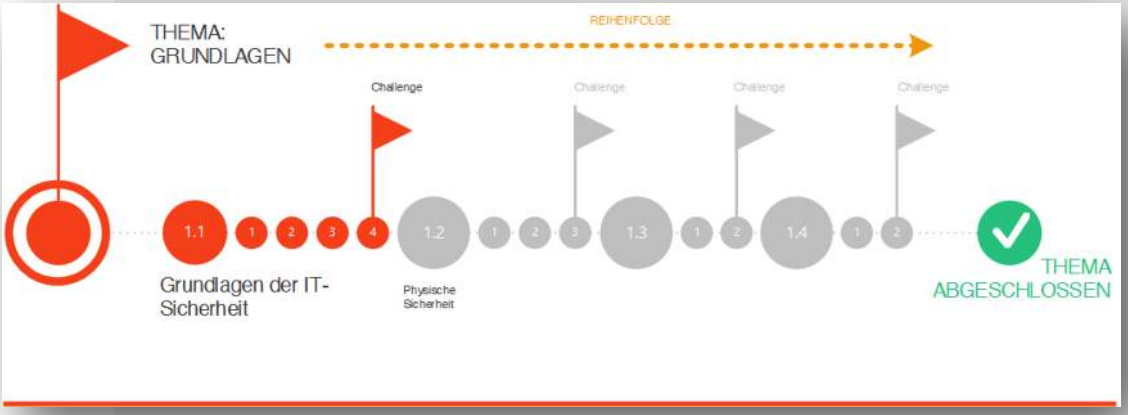
03 Aufbereitung der Lerninhalte in Lernpakete

Sinnvollerweise sollten die unterschiedlichen Lerninhalte in „verdaubaren Häppchen“ serviert und auch nur den entsprechenden Zielgruppen zur Verfügung gestellt werden, die diese für ihre täglichen Aufgaben benötigen.

An dieser Stelle ist es zu vermeiden, die Mitarbeiter:innen mit Regularien, Hinweisen und Aufgaben zu überfordern bzw. Inhalte zu vermitteln, die weder im Büroalltag noch im privaten Umfeld nützlich sind.

04 Aufteilung in unterschiedliche Schwierigkeitsgrade

Damit Mitarbeiter:innen möglichst effektiv an notwendige Inhalte gewöhnt werden, sollten die Module innerhalb des Themenbereiches entsprechend der Vorkenntnisse vermittelt werden, heißt konkret: es sollten ***Basis-Module*** geschaffen und anschließend über ***Aufbau-Module*** intensiviert werden. Grundsätzlich sollten Aufbaukurse erst nach erfolgreicher Absolvierung des Basis-Moduls verfügbar sein. So kann sichergestellt werden, dass alle Teilnehmer:innen den Inhalten folgen und die Lernziele erreichen können.



05 Effektive Wissensvermittlung

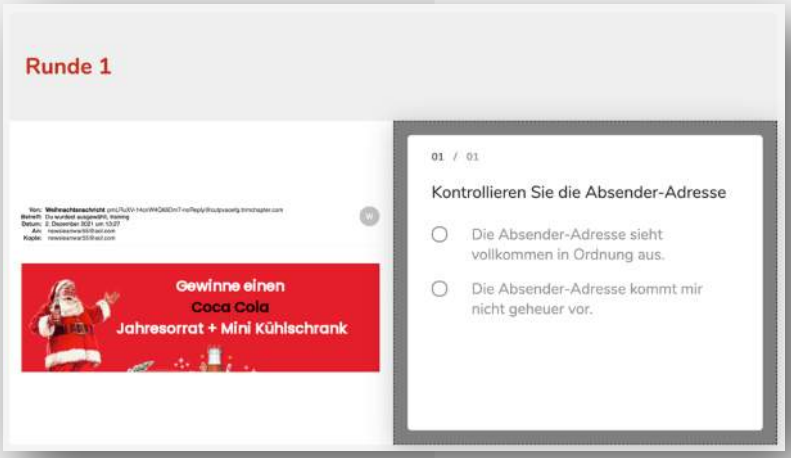
Aus den genannten Punkten lässt sich ableiten, dass die Bearbeitung der Lernmodule in einer überschaubaren Zeit mit einer Vermittlung der Themenschwerpunkte möglich sein sollte. Die Effektivität lässt sich mit einer unmittelbaren Lernerfolgsmessung ermitteln.

An dieser Stelle haben sich sogenannte WBT (Web Based Trainings) bewährt, die u. a. folgende Vorteile mit sich bringen:

- Kleine Micro-Learnings (Dauer zwischen 3 - 6 Minuten) greifen ein spezifisches Thema konzentriert auf
- Kleine Einheiten können bei Bedarf jederzeit zur Wiederholung aufgerufen werden
- Alle können den idealen Zeitpunkt für ihr eigenes Training selbst wählen
- Spielerische Formen können die Mitmachbereitschaft deutlich steigern
- Inhalte lassen sich leicht ergänzen bzw. überarbeiten
- Einfache Kontrollmöglichkeiten für die Geschäftsleitung

Ein hoher Praxisanteil innerhalb der WBT-Module unterstützt, die Awareness-Kampagnen aufzulockern:

- Kurze Quizfragen
- Umfragen zum aktuellen Thema
- Gezielte Fragen zu den Inhalten
- Interaktive Elemente



Neben den WBT können auch weitere Schulungsmaßnahmen das notwendige Wissen aufbauen und das Verständnis fördern:

- Präsenzschulungen
- Live-Hacking Vorführungen
- Online-Videos
- Handouts

06 Wiederkehrende und messbare Maßnahmen

Ziel dieses Schrittes ist es, das hohe Niveau der IT-Security-Awareness durch regelmäßige Maßnahmen aufrecht zu erhalten. Erfahrungsgemäß lässt erzieltes Sicherheitsbewusstsein nach kurzer Zeit wieder nach. Zudem führen auch neue oder geänderte IT-Services neue Gefahren mit sich.

Denkbare Maßnahmen könnten sein:

- Phishing-Simulationen für zufällig ausgewählte Mitarbeiter:innen
- Simulierte Anrufe zur Datenauskunft
- „Tür-Anhänger“, wenn Mitarbeiter die Büros nicht verschließen
- Fortsetzungsquiz oder Rätsel
- Artikel im Intranet oder in einer Mitarbeiterzeitung

Zudem können auch Materialien verwendet werden, die bereits unter Punkt „*02 Bekanntmachung*“ eingesetzt wurden.

Damit sich das Management einen Überblick über die Awareness-Kampagne und den Trainingserfolg bilden kann, können technische Kennzahlen erfasst und analysiert werden. Beispiele dafür sind:

- Geöffnete E-Mails aus den Phishing-Simulationen
- Zugriffsversuche auf kritische Webseiten
- Anzahl der eingehenden / gefilterten / geöffneten SPAM-E-Mails
- Punktzahl durchgeführter Awareness-Challenges

Mögliche Inhalte einer Awareness-Schulungen

Teilweise versuchen Organisationen mit ihren Unterlagen auch Kompetenzen mit real gewordenen Bedrohungen zu vermitteln. Was dabei jedoch häufig übersehen wird ist, dass die Angriffe für „nicht-IT'ler" kaum nachvollziehbar sind. Somit sollten diese komplexen Abläufe auch nicht Ziel einer Security-Awareness-Kampagne sein. Vielmehr gilt es die Prävention in den Vordergrund zu stellen.

Folgend ein kleiner Auszug möglicher Schulungsschwerpunkte:

- ❑ Grundsätzliche Definitionen und Erklärungen zu IT-Security-Themen
  (Physische Sicherheitskomponenten, Grundlagen zur elektronischen Kommunikation, Allgemeine Bedrohungen, Verhalten am Arbeitsplatz)
- ❑ Passwortverwaltung
  (Sicherheit bei Passwörtern, Passwortgeneratoren und -tresore, Sichere PINs, Multi-Faktor-Authentifizierung)
- ❑ E-Mail-Sicherheit
  (E-Mails auf mobilen Geräten, Einsatz von Tools zum Absichern von E-Mails, Anhänge und deren Gefahren)
- ❑ Phishing
  (Typische Warnsignale, Spear-Phishing, Fraud-Attacken)
- ❑ Mobile Geräte
  (Sicherheit bei mobilen Geräten, beim Einsatz von Apps und auf Reisen)
- ❑ Web-Browsing und Internet
  (Sicheres Surfen im Internet, Gefährliche URLs und Erkennen von Gefahren, Cloud-Services)
- ❑ Social-Media
  (Betrügereien auf Social-Media-Plattformen, Sichere Nutzung von Social Media)
- ❑ Datenschutz
  (Überblick über die DSGVO und die Berührungspunkte zur Informations-sicherheit, Sicheres Vernichten von Informationen)
- ❑ Ggf. weitere Themen
  (Sicherheit im Gesundheitswesen, PCI-DSS, IoT, etc.)

Mitarbeiter-Awareness | Aktivieren Sie die menschliche Firewall

Bezugnehmend auf den Titel dieser Broschüre „Mitarbeiter-Awareness | Aktivieren Sie die menschliche Firewall“ ist es sehr schwer, sein Personal zu einem „Schutzschild gegen Cyberangriffe“ zu machen.

Allerdings wäre es fahrlässig, es nicht mindestens zu versuchen, da ein kleiner Fehler eines Einzelnen unendlich viele Folgen für das komplette Unternehmen nach sich ziehen könnte.

Beispielsweise könnte die Unachtsamkeit beim Öffnen einer einzigen E-Mail einen Prozess anstoßen, der alle Daten im Unternehmen, in allen Zweigstellen und in der Cloud innerhalb von nur wenigen Sekunden verschlüsselt. Keiner könnte mehr arbeiten, die Produktion wäre sofort stillgelegt und die finanziellen Folgen können für das Unternehmen existenzbedrohend sein. Hinzu kämen datenschutzrechtliche Meldepflichten, die fast unvermeidlich einen Imageschaden nach sich ziehen.

Mitarbeiter-Awareness | Lösungen

Ob, zusätzlich zu allen möglichen technischen Voraussetzungen, kontinuierliche Präsenzschulungen Ihres Personals, Web Based Trainings, Online-Trainings oder eine eigens für Sie entwickelte Sicherheitsstrategie die richtige Lösung für Ihr Unternehmen ist, müssen Sie entscheiden. Wir können Sie an dieser Stelle nur soweit unterstützen, mit Ihnen gemeinsam alle Möglichkeiten zu diskutieren und für Sie und Ihr Unternehmen ein maßgeschneidertes Sicherheits-Konzept zusammenzustellen, bei dem das Thema Mitarbeiter-Awareness eine maßgebliche Rolle spielt.

Mitarbeiter-Awareness | Fazit

Aufgrund der stetig steigenden Cyberangriffe und der Gefahr durch immer mehr *Social-Engineering-Angriffe*, ist es für jedes Unternehmen unabdingbar, sein Personal auf die möglichen Gefahren hinzuweisen - alle Mitarbeiter:innen kontinuierlich über neue Angriffsmethoden zu informieren und stetig alle zu sensibilisieren, sprich das Thema Mitarbeiter-Awareness fest in alle Prozesse zu integrieren.

Oktober | 2022

Impressum

CS Hard- & Software Consulting GmbH
Saarbrücker Straße 72
66386 St. Ingbert
Tel.: 06894 - 38797 - 0
Fax: 06894 - 38797 - 99
Web: www.compusaar.de
E-Mail: info@compusaar.de

Amtsgericht St. Ingbert / HRB13312
Ust.-ID-Nr.: DE813536236
p.h.G.: CS Hard- & Software Consulting GmbH
Geschäftsführer: Ursula Doll

Redaktion
Alexander Eich

Bildnachweise
Diese Unterlage wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausen erstellt. Einige der dargestellten Bilder wurden von der ITKservice bei https://www.ccvision.de gekauft und lizensiert. Weitere stammen von https://pixabay.com/de/ einer Plattform für