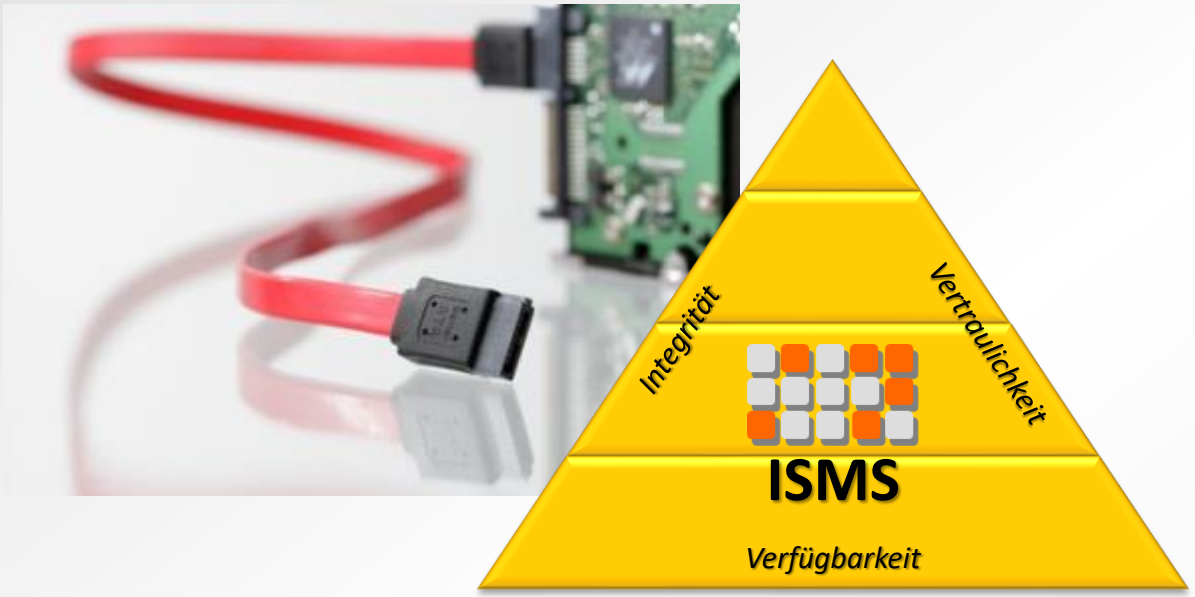


e.solutions Partnernetzwerk

Schulung zur Informationssicherheit

Agenda

1) **Motivation der Informationssicherheit**
2) **Was ist Informationssicherheit?**
3) **ISMS-Organisation, ISMS Policies, Scope**
4) **Gefährdungen und Angriffsziele**
5) **Best Practice**
6) **Phishing**
7) **Social Engineering**
8) **Prototypenschutz**
9) **Meldung Sicherheitsvorfälle**

e.solutions

Motivation

- **Verschärfte Sicherheitslage!**

  Aktuelle Angriffsvorfälle (Komplexität & Häufigkeit)

- **Wachsende Komplexitäten!**

  Schnittstellen (intern / extern / international)

- **Auditanforderungen zur Informationssicherheit (TISAX VDA ISA)**

Was ist Informationssicherheit?

Begriffsdefinitionen

Informationssicherheit	IT-Sicherheit	Datensicherheit	Datenschutz

▪ Schutz der CIA Prinzipien
▪ Informationen
  ▪ in allmöglichen Formen
  ▪ auf verschiedenen Systemen
▪ Technische und organisatorische Schutzmaßnahmen
  ▪ ISMS Organisation
  ▪ Richtlinien
  ▪ Audits
	▪ Schutz der IT-Systemen
	▪ Teilbereich der Informations-sicherheit
	▪ Technische Schutzmaßnahmen
	  ▪ Firewall
	  ▪ Verschlüsselung
	  ▪ Antivirus
		▪ Schutz von Daten
		  ▪ Verlust
		  ▪ Verfälschung
		  ▪ Beschädigung
		  ▪ Wiederherstellung
		▪ Teilbereich der Informations-sicherheit
		▪ Beispiele
		  ▪ Backup
		  ▪ Datenmaskierung
		  ▪ Datenlöschung
			▪ Schutz von personenbezogenen Daten
			▪ EU-DSGVO (Datenschutz Grundverordnung)
			▪ Beispiele
			  ▪ private Anschrift
			  ▪ Geburtsdatum
			  ▪ biometrische Daten

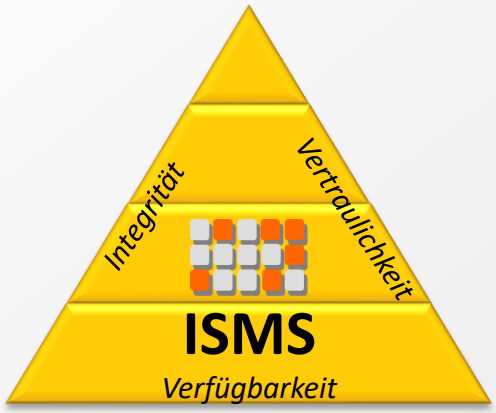
e.solutions

Informationssicherheit

- „**need-to-know**“ Prinzip

- Sicherstellung der **Schutzziele** (CIA Prinzip)
  - Vertraulichkeit von Informationen (Confidentiality)
  - Integrität von Informationen (Integrity)
  - Verfügbarkeit von Informationen (Availability)

- **Schutz** vor
  - unbefugten Zugriff
  - Manipulation
  - Sabotage
  - wirtschaftlichen Schäden



Informationssicherheits-Organisation
ISMS Policies
Scope

Informationssicherheits-Organisation
ISMS Policies

- Der **CISO** (Chief Information Security Officer) und das **Informationssicherheits-Team** definieren, implementieren, kontrollieren und optimieren das ISMS in einem kontinuierlichen Verbesserungsprozess.
- Unterschiedliche **Richtlinien** und **Leitlinien** sind geschrieben, um das ISMS aufrecht zu halten und zu regeln.
- Es erfolgen daher in regelmäßigen Abständen **Überprüfungen** und **Aktualisierungen** der ISMS Dokumentation und Prozesse sowie des Informationssicherheits-**Risikomanagements**.
- Falls Sie weitere Fragen zur Informationssicherheit oder zu Audits haben, können Sie uns per **E-Mail** gerne erreichen:

Email Informationssicherheits-Team
eso.group.informationssicherheit@esolutions.de

Scope

- TISAX (Trusted Information Security Assessment Exchange)
  - definierter Standard der Automobilindustrie für Informationssicherheit
  - von ISO 27001 abgeleitet
  - seit 2017 müssen alle Unternehmen nach TISAX geprüft sein, wenn sie mit OEMs u. Kunden der deutschen Automobilindustrie arbeiten
- TISAX Label für alle e.solutions GmbH Standorte
  - Erlangen: Info High, Proto-Parts & Components, Data Protection
  - Ingolstadt: Info High, Proto-Parts & Components, Data Protection

Gefährdungen und Angriffsziele auf die Informationssicherheit

Sicherheitsthemen im Alltag

E-Mail

- Zugriff auf Mailbox von Kollegen
- Weiterleitung
- Verschlüsselung von E-Mails an Kunden
- Signierung von E-Mails
- Weitergabe von Kontaktinformationen

Daten

- Zugriffsschutz
- Soziale Netzwerke
- Umgang mit Passwörtern
- USB-Sticks und andere Datenträger
- Datensicherung
- Archivierung

Schutzziele

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Sprache / Voice

- Schutz vor Mithörern
- Abhörsichere Konferenzen
- Social Engineering
- Weitergabe von Kontaktinformationen

Papierunterlagen

- mobiler Arbeitsplatz
- Drucken
- Postversand
- Konferenzräume
- Datensicherung
- Vernichtung

e.solutions

Best Practices

Ausweistragepflicht!

Niemand darf ohne Ausweis oder Begleitung ins Gebäude

e.solutions

Klassifizierung der Informationen!

Klassifiziere die Daten und behandle sie entsprechend!

- ***Öffentlich***

  (z. B. Informationen der eso-Homepage)
- ***Intern***

  (z. B. Organigramm, Firmenkennzahlen)
- ***Vertraulich***

  (z. B. Produktionsplanung, Releasepläne)
- ***Streng Vertraulich***

  (z. B. Prototypen, Code)

e.solutions

Schutz von Informationen

- *hier: Dokumente und Speichermedien*
- *Nichts herumliegen lassen, was Firmenfremde nichts angeht*
- *Bewahre e.solutions Geräte und Dokumente sicher auf*
- *Vernichte Dokumente nach Gebrauch*
- *Lösche e.solutions Medien nach Absprache mit uns*
- *Drucker nach Papierende auffüllen*
  - *Ansonsten kommt der Druckauftrag beim nächsten User heraus!*

e.solutions

Schutz vor ungebetenen “Gästen”

- *Stoppe Personen, die **unbekannt** sind oder die sich nicht ausweisen können schon an der Gebäudetür (Höflich sein, aber bestimmt.)*
- *Dokumentiertes **Besuchermanagement** ist empfehlenswert*
  - *Beispiel:*
    - *Besucherliste am Empfang*
    - *Besucherausweis*

e.solutions

SmartCard

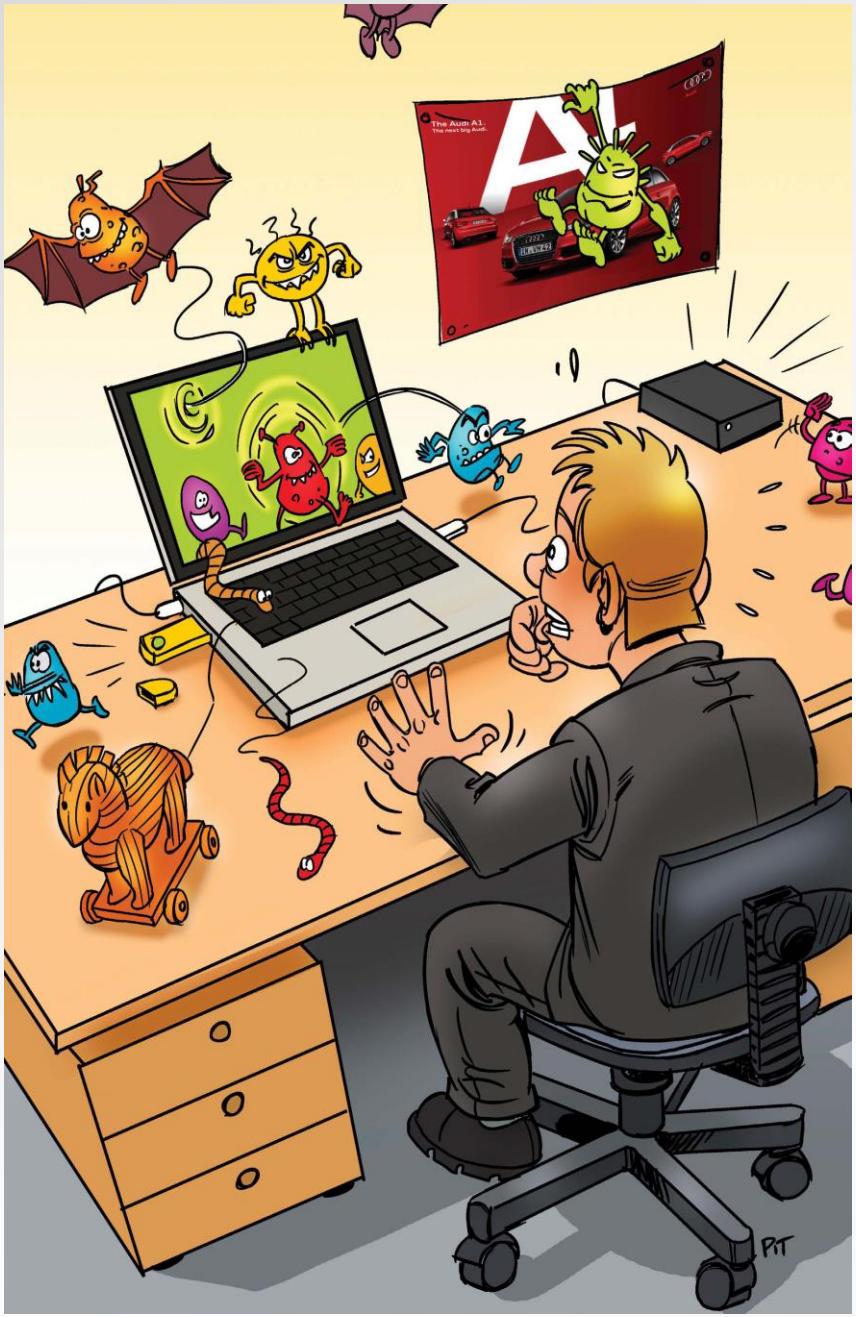
- *Login & Passwort sind eine **1-Faktor-Authentifizierung:** Nur Wissen*
- *SmartCard & PIN sind eine **2-Faktor-Authentifizierung:** Wissen & Besitz*
  - *Die Karte ist der erste Faktor*
  - *Die PIN ist der zweite Faktor*
- *Sicherer Umgang mit **Passwörtern***
- ***Aufbewahrung SmartCard***
  - *getrennt vom Rechner*
  - *Stets im persönlichen Zugriff: Beim Verlassen des Rechners mitnehmen – immer!*

e.solutions

Trennung Arbeit/ Privat

- *Keine private Musik, Hörbücher, Online-Streaming, etc. auf e.solutions Arbeitsgeräten*
- *Keine illegalen Downloads*
- *Kein Peer-2-Peer Sharing*
- *Keine Browser-Plugins zur Synchronisation (Google Chrome: Plugin synchronisierte alle privaten Downloads auf dem e.solutions Arbeitsgerät!)*
- *Keine Firmendaten auf privaten Geräten*
- *Keine Cloud-Dienste zur Synchronisation oder Speicherung*

e.solutions



Erst denken, dann klicken!

- *Downloads nur aus sicheren Quellen*
- *Vorsicht bei*
  - *unbekannten, unerwarteten Dateien*
  - *Unerwarteten E-Mails*
- *Scan von fremden Datenträger*
  - *Rechte Maustaste – Scan with ESET*

e.solutions

Vorsicht! Kryptotrojaner!

- *Mailanhang enthält Downloader und lädt den Kryptocode nach*
  - *Kryptotrojaner verschlüsselt im Hintergrund alle im Zugriff befindlichen Dateien (Lokale und Netzlaufwerke!)*
  - *Irgendwann bootet das System mit einer Erpressungsmeldung*
- *Mailanhänge als Rechnung, Lieferschein, Zustellbestätigung, etc. getarnt*
- *Absender häufig gefälscht– kann auch @esolutions.de sein!*
- ***Aufmerksamkeit ist das wirksamste Mittel.***

e.solutions

E-Mail Verschlüsselung

- *Bitte den Informationsaustausch per E-Mail verschlüsseln*
  - ***Mindestanforderung** von VDA ISA ist mandatoryTLS bei hohen Schutzbedarf*
  - *Voraussetzung, eso.IT und Partnerfirmen haben Verfahren beidseitig implementiert.*
- *Mit einigen Firmen hat eso. den Kommunikationsweg mittels mandatoryTLS gesichert.*

e.solutions

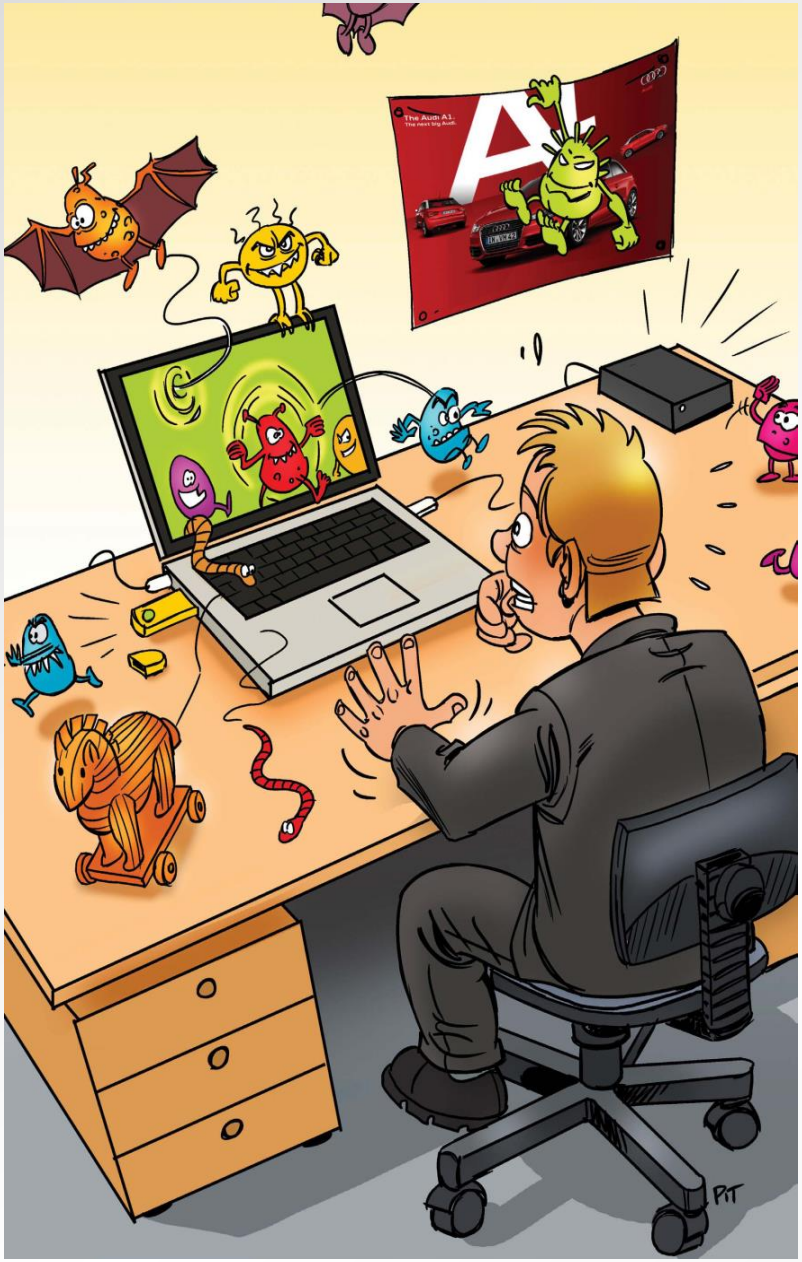
Clean Desk Policy

- Vor Feierabend Arbeitsplatz aufräumen
- Vertrauliche Dokumente und Geräte in abschließbaren Schränke, usw. aufbewahren
- Keine Sticky-Notes mit vertraulichen Informationen z.B. auf den Tisch kleben
- Keine USB-Sticks oder andere mobile Endgeräte auf dem Tisch liegen lassen
- Nicht verwendbare Unterlagen, unbekannte Datenträger, etc. in Shredder bzw. Vernichtungscontainer entsorgen

➤ Ziel: ISO 27001 und DSGVO konform

e.solutions

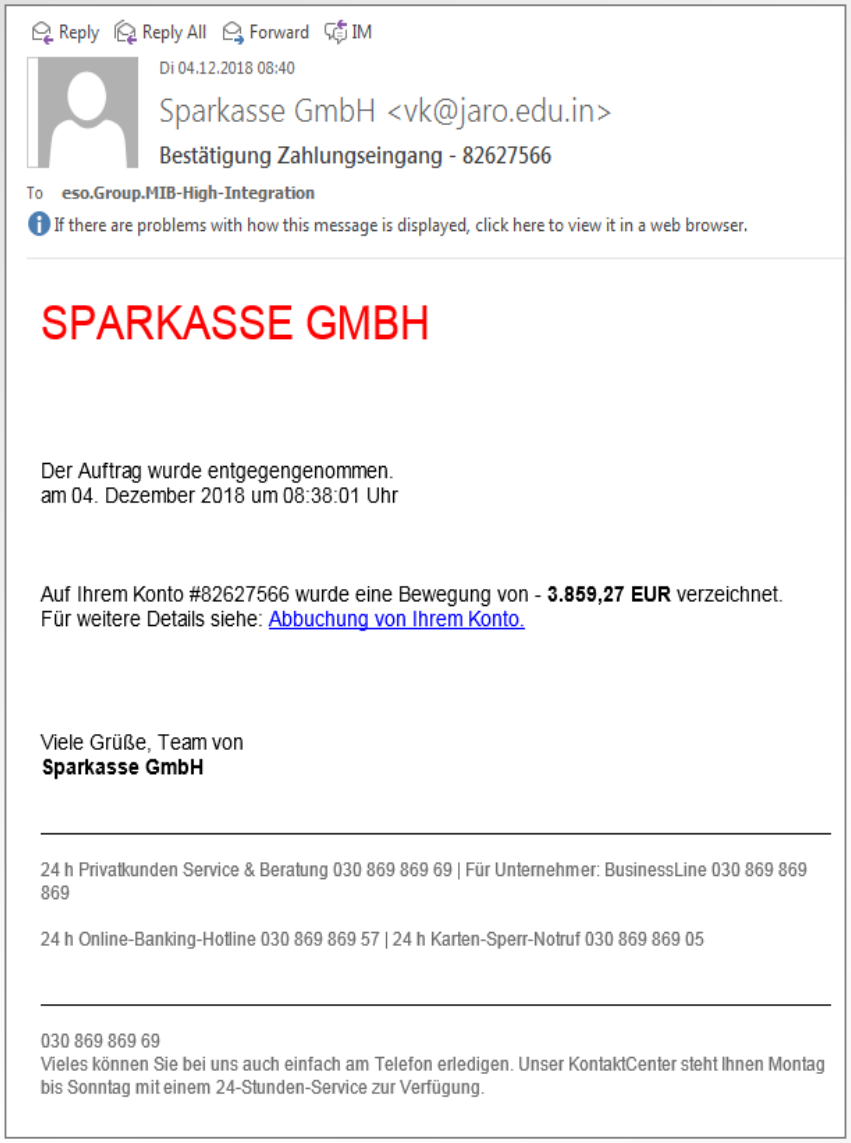
Umgang mit Phishing



Vorsicht! Phishing E-Mail!

- *Mailanhang enthält Hinweis auf*
  - *z. B. einen Mangel und fordert zu einer Aktion auf*
- *Keine Makros aktivieren*
- *Link auf eine Fake Seite zur Eingabe von Daten*
  - *Erkennbar z.B. durch MouseOver auf den Link*
- *Diebstahl der Daten durch Eingabe dieser auf einer Fake Seite*
  - *Erkennbar z.B. anhand des Domain-Namen*

Wie erkennt man eine Phishing E-Mail?



Reply Reply All Forward IM

Di 04.12.2018 08:40

Sparkasse GmbH <vk@jaro.edu.in>

Bestätigung Zahlungseingang - 82627566

To eso.Group.MIB-High-Integration

If there are problems with how this message is displayed, click here to view it in a web browser.

SPARKASSE GMBH

Der Auftrag wurde entgegengenommen.
am 04. Dezember 2018 um 08:38:01 Uhr

Auf Ihrem Konto #82627566 wurde eine Bewegung von - **3.859,27 EUR** verzeichnet.
Für weitere Details siehe: Abbuchung von Ihrem Konto.

Viele Grüße, Team von
Sparkasse GmbH

---

24 h Privatkunden Service & Beratung 030 869 869 69 | Für Unternehmer: BusinessLine 030 869 869 869

24 h Online-Banking-Hotline 030 869 869 57 | 24 h Karten-Sperr-Notruf 030 869 869 05

---

030 869 869 69
Vieles können Sie bei uns auch einfach am Telefon erledigen. Unser KontaktCenter steht Ihnen Montag bis Sonntag mit einem 24-Stunden-Service zur Verfügung.

Hinweise

- *Nicht-personalisierte Anrede*
- *Unpassende Absenderadresse*
- *Knappe Frist*
- *Anfrage an Anmeldedaten, PIN*
- *Unterschiedliche Schriftarten und Schriftgrößen*
- *Grammatik- und Rechtschreibfehler*
- *Link oder Anhang*

Handlungsanweisung

- *Nirgends hinklicken*
- *Screenshot der Mail an eso.group.CERT@esolutions.de*
- *Dann Mail löschen! (SHIFT+DEL)*
- *Falls, die E-Mail, Link oder Anhang geöffnet, wurde, **sofortige Meldung** an*
  1) *Vorgesetzten*
  2) *eso.group.CERT@esolutions.de*
  3) *Ihre IT /IT-Sicherheit*

e.solutions

Umgang mit Social Engineering!

Was ist Social Engineering!

- *Eine Art Manipulation oder Täuschung über die Absicht o. die Identität des Täters*
- *Zwischenmenschliche Beeinflussung mit dem Ziel, vertrauliche Informationen zu erwerben*
- *Beispiele:*
  - *Telefonanrufe*
  - *Emails / Phishing*
  - *Scareware*

Handlungsanweisung

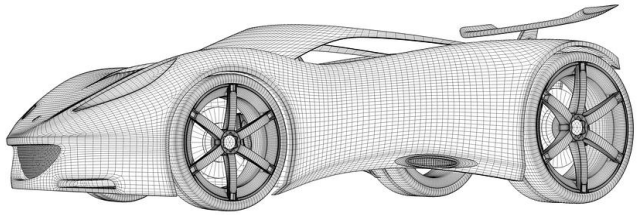
- *Keine Rufnummer von Vorgesetzten u. Kollegen weiterleiten*
- *Keine interne Informationen mitteilen*
- *Keine Mitarbeiter-Namen, Handynummer, E-Mail Adresse, usw. mitteilen*
- *Name des Anrufers und der Rufnummer notieren*
- *Meldung an*
  1) *Vorgesetzten*
  2) *eso.group.CERT@esolutions.de*
  3) *Ihre IT /IT-Sicherheit*

e.solutions

Umgang mit Prototypenschutz

Prototypen-, Komponentenschutz nach TISAX

- *Schutzbedarf von Prototypen, Bauteilen oder Komponenten muss vom Auftraggeber definiert sein*
- *Mitarbeiterschulungen zum Umgang mit Prototypen, Bauteilen oder Komponenten sind durchzuführen*
- *Einhaltung des Schutzbedarfs wird auditiert*



Handlungsanweisung

- *Prototypenfahrzeuge/-Komponenten; Erprobungsfahrzeuge*
  - *Abstellen in Projekträume (mit abgesperrter Plane) bzw. gesicherte Stellflächen (Videoüberwachung)*
  - *Fahrzeuge durch Auftraggeber bereits getarnt (z.B. Folie)*
  - *Transport in verplombten LKWs bzw. in Transportboxen vom Auftraggeber*

- *Sicherung der Räumlichkeiten*
  - *Dokumentiertes Besuchermanagement bzw. Schlüsselmanagement und Zutritts- und Zugangsregelung*
  - *Sicherung vor unbefugten Eintritt durch Einbruchmeldeanlage (Bewegungsmelder)*
  - *Einsatz vom Rauchmeldern im Flur, Technikräumen, Räume der Elektroversorgung, Entwicklungsräumen*
  - *Schilder des Fotografieverbotes*

e.solutions

Meldung von Sicherheitsvorfällen!

Sicherheitsvorfall / Security Incident

Was ist ein Sicherheitsvorfall?

potenzielle oder reale Gefährdung

..... schutzbedürftiger .....

Information, Räume, Systeme

- Kriminelle Handlungen
- Benutzerfehlverhalten
- Technische Sicherheitslücken

Beispiel

- gestohlenes Notebook/ Smartphone
- verschwundene Teile
- unberechtigte Personen in Gebäude
- Schadsoftware
- Social Engineering (Anruf / Phishing)

e.solutions

Sicherheitsvorfälle Melden

eso.group.CERT@esolutions.de

Bitte senden Sie uns bei Verdachtsfällen zum Thema Information-/ IT-Security umgehend eine Email

Vielen Dank für die Teilnahme

und Ihre Aufmerksamkeit!

Information Security Is Everyone‘s Responsibility

e.solutions