Erwischt!
Ein Betroffener berichtet über eine Ransomware-Attacke

Werner Grohmann:

- Geschäftsführer GROHMANN BUSINESS CONSULTING
  - Redaktion und Marktforschung für deutsche und internationale IT-Anbieter
  - Hybrides Beschäftigungsmodell (Feste/freie Mitarbeiter)
  - Hybrides Arbeitsplatzmodell (Büro/Home Office)
- „Digital Immigrant“
  - Klassische IT-Infrastruktur (MS-Office, Grafikprogramme, CRM, CMS, Programmier-Tools, etc.)
  - Cloud Computing-Liebhaber (Collaboration-Plattform, Online-Umfragetool, Cloud Backup, DATEV Cloud)
  - Datenschutz/Datensicherheit „auf dem zweiten Bildungsweg“
  - „Was gibt es bei uns schon zu holen?“

E-Mail einer PR-Agentur an mich:

„Leider wurde eine Mitarbeiterin unseres Unternehmens Opfer eines Phishing-Angriffs.

Als Resultat hatten Dritte kurzzeitig die Möglichkeit, als Rechnungsvorgang getarnte Phishing-Mails zu verschicken.“

Nachfrage bei der Buchhalterin:

„Habe nachgeschaut. Nichts offen …“

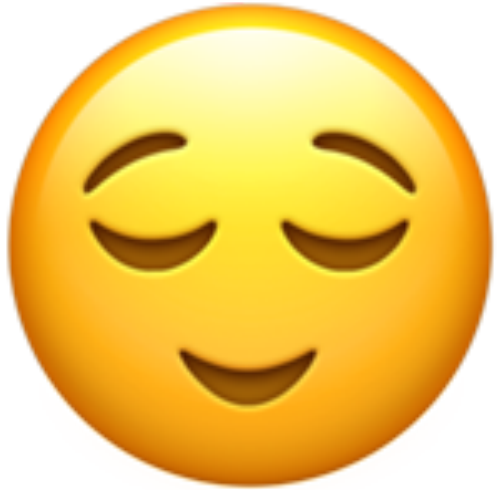
Weiterer Ablauf

- Die nächsten Tage läuft alles wie bisher
- Einige Tage nach der E-Mail: Ransomware-Attacke
  - Alle zugänglichen Systeme sind verschlüsselt
  - Bildschirme zeigen die Lösegeldforderung in Bitcoins
  - Komplette Hilflosigkeit („Was müssen wir jetzt tun?“)
- Die folgenden zwei Wochen
  - Komplette IT offline: Kein lokales Arbeiten möglich
  - Arbeiten über Cloud-Lösungen möglich/Keine Kundendaten betroffen
  - Neue Hardware wird beschafft
  - Systeme werden aus Cloud-Backups wiederhergestellt

Bilanz

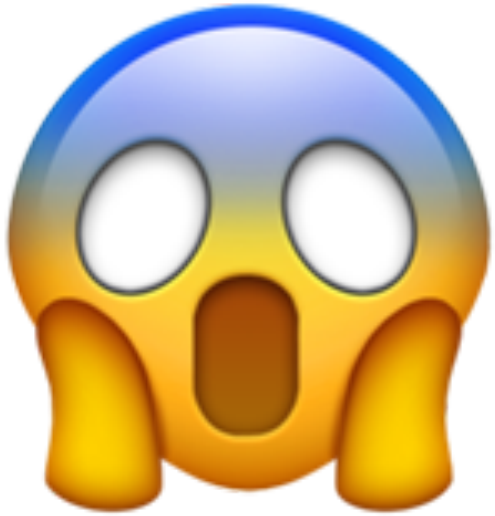
- Gesamtkosten: 28.000 Euro (Hardware, Dienstleistungen, Arbeitszeit)
- Arbeitsausfall: ca. zwei Wochen

Mein Wechselbad der Gefühle



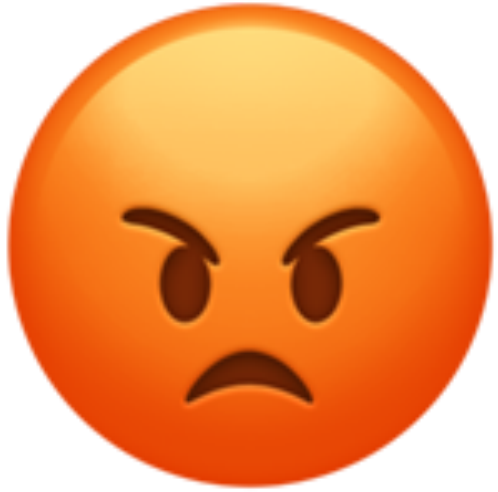
Gott-sei-Dank: (Wohl) nix passiert!

Mein Wechselbad der Gefühle



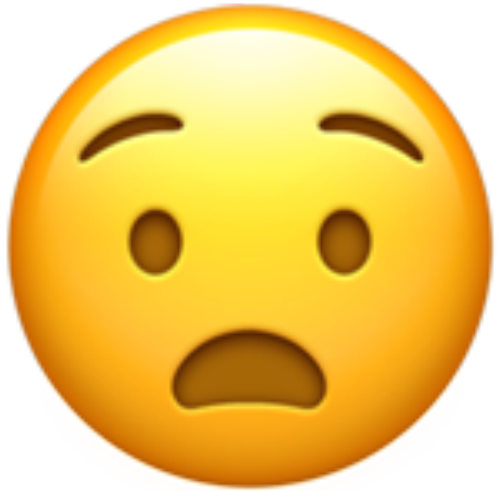
Ach du große Sch …!!!!

Mein Wechselbad der Gefühle



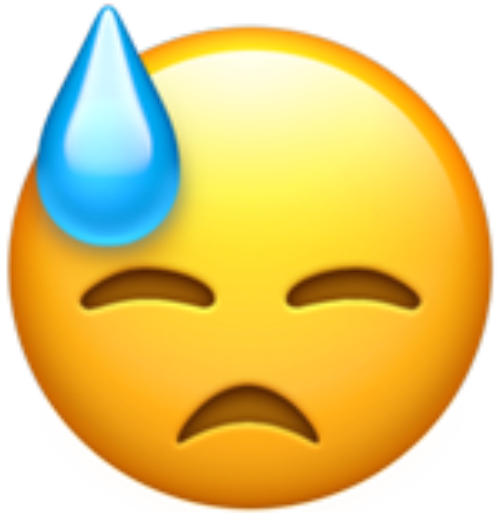
Wie kann man denn nur so blöd sein …?

Mein Wechselbad der Gefühle



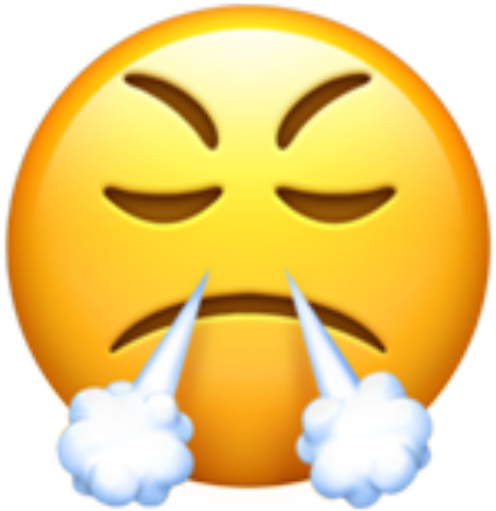
War‘s das jetzt mit GROHMANN BUSINESS CONSULTING …?

Mein Wechselbad der Gefühle



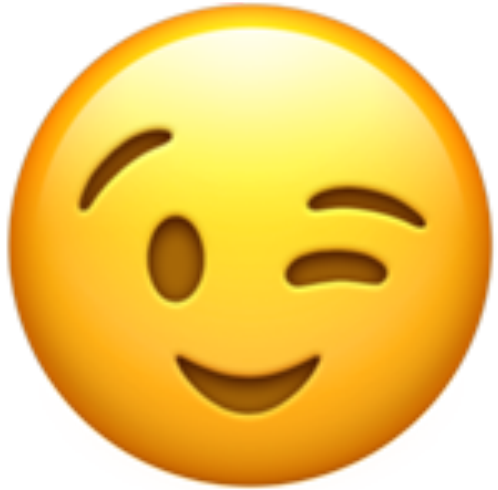
Wann wird alles wieder so wie früher …?

Mein Wechselbad der Gefühle



So ein A …?

Mein Wechselbad der Gefühle



Uff! Alles wieder am Laufen …

Noch einmal Glück gehabt, andere hatten da weniger Glück

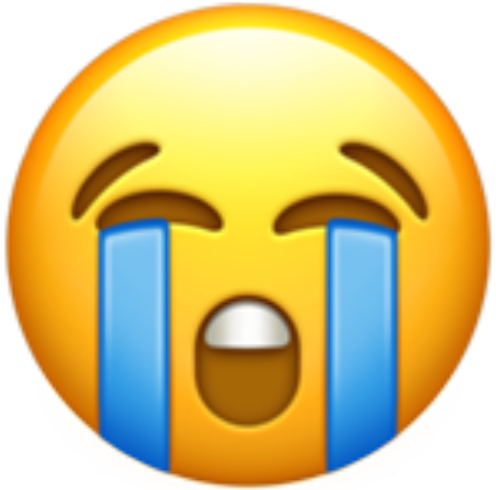
Die Schumag AG ist Opfer eines Cyberangriffs geworden. **Das Unternehmen hat deshalb seine Hauptversammlung abgesagt.**

Verschlimmerte Lage durch Cyberattacke: **Traditionsunternehmen mit über 400 Beschäftigten ist insolvent.**

Unico Data: Cyberangriff führt zu **Vertrauensverlust** und letztendlich zu **Aufgabe des Geschäftsbetriebs**

Familienunternehmen meldet nach Hackerangriff Insolvenz an

Reaktion unserer Buchhalterin



Hätte ich da bloß nicht draufgeklickt!!

Zahlen und Fakten – Der Faktor Mensch

- **70% der erfolgreichen Cyberattacken** beginnen mit **einer Phishing-E-Mail, die nicht als solche erkannt wird**
- **95% aller Verstöße gegen die Cybersicherheit** basieren auf **menschlichem Versagen**
- **88% aller Datenschutzverletzungen** sind auf **Mitarbeiterfehler** zurückzuführen
- **57 % aller Mittelständler mit 50 bis 250 Mitarbeitenden** waren **schon mindestens einmal** von einer Cyber-Attacke betroffen.
- **Durchschnittliche Schadenshöhe** bei einem Cyber-Angriff: **95.000 €**

Quellen: GDV, HDI, ENISA,

Zahlen und Fakten – Fremdbild vs. Selbstbild

- **80% der KMUs** sehen ein hohes Cyberrisiko für andere Unternehmen, aber nur **34% glauben, selbst gefährdet zu sein.**
  - „Das trifft doch nur die Großen …!“
  - „Was soll bei uns schon zu holen sein …“
- **77%** glauben, sie tun genug – doch **nur ein Drittel** hat die wichtigsten Sicherheitsmaßnahmen implementiert
- **64%** der Unternehmen **verzichten komplett** auf **Mitarbeiterschulungen**

Quelle: GDV

BSI-Lagebericht zur IT-Sicherheit in Deutschland

- KMU im Visier von Cyberangreifern
  - BSI: „Ziel muss es sein, Cybersicherheit auch bei KMU auf die Agenda zu setzen und als unternehmensweites Risiko zu betrachten – und dies am besten ausgehend von der Unternehmensleitung.“
- Das trifft doch nur die Großen
  - BSI: „Cyberkriminelle allerdings gerne nach dem Motto ‚minimaler Aufwand, maximaler Ertrag‘. Über den Weg des geringsten Widerstandes schlagen diese vor allem gerne bei KMU zu.“
- „Das wir schon irgendwie selbst hin“
  - Laut BSI-Ansatz in vielen Unternehmen
  - Mangel an Budget, Kapazitäten (IT-Fachpersonal), Bewusstsein

BSI-Lagebericht zur IT-Sicherheit in Deutschland:

Gefährdungslage insbesondere durch Ransomware

„besorgniserregend“

Wie gelingt es, das **Bewusstsein im Unternehmen** für die **Risiken und Gefahren** in den **Bereichen Datenschutz und Datensicherheit** zu wecken bzw. zu schärfen?

Risikofaktor Mensch

vs.

„Human Firewall“

Security Awareness Programm - Ablauf

12 Monate

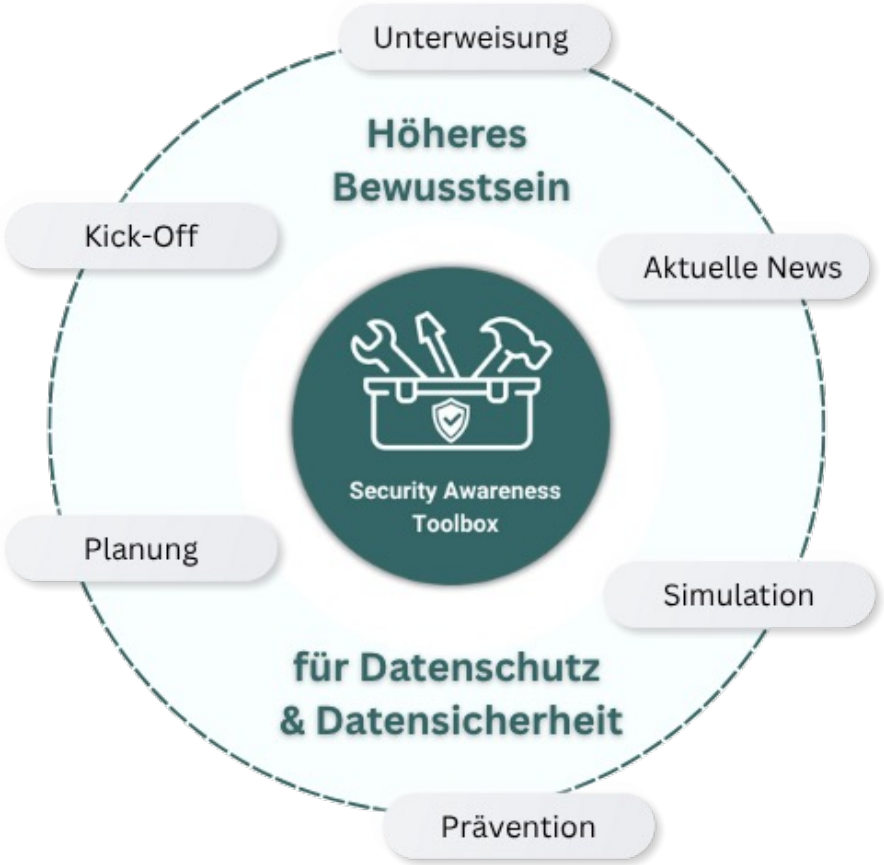
Security Awareness Programm – Formate

- Kickoff-Meeting
  - Startschuss für Security Awareness Programm
- Regelmäßige Security Awareness-Kampagnen
  - Schulungen (Sichere Passwörter, Social Engineering, Phishing-Beispiele)
  - Newsletter (Aktuelle Bedrohungen, Tipps für die tägliche Arbeit)
  - Quiz/Test (Interaktion, Überprüfen des Lernerfolgs)

Security Awareness Programm – Erkenntnisse

- Security Awareness ist ein kontinuierlicher Prozess
  - Immer neue Bedrohungen
  - „Vergessenskurve“ (Ebbinghaus)
- Kampagnen-Regelmäßigkeit ist zentraler Erfolgsfaktor
  - Kontinuierliche Teaser
  - Unterschiedliche Formate wichtig
- Security Awareness ist keine Frage von Alter und Geschlecht
  - „Alte“ und „Junge“ genauso anfällig
  - Unterschiedliche Angriffsszenarien
- Security Awareness Programm lohnt sich!

Ergebnis unserer Erkenntnisse: Ohne Bewusstsein keine Sicherheit



Kontaktdaten

Werner Grohmann

Tel.: +49 (0) 761 2171 6068

E-Mail: wgrohmann@grohmann-business-consulting.de

Internet:

www.grohmann-business-consulting.de

www.security-awareness-toolbox.de