Unterweisung Informationssicherheit

Michael Traxler

GRUNDIG
Business Systems

Juni 2024

Einführung

Geltungsbereich

- für alle Mitarbeiter von GBS-Audio und der GBS ES
- für die Standorte Bayreuth, Nürnberg und mobiles Arbeiten
- für alle digitalen und analogen Daten

Einführung

Statement der Geschäftsführung

Unsere Geschäftsführung unterstützt und trägt vollständig alle Informationssicherheitsmaßnahmen.

Einführung

Klassifizierung der Informationen

- Unklassifizierte, öffentliche Informationen
  - unsere Webseiten, Public-Ordner
- Informationen für interner Gebrauch
  - SharePoint, Teams, Laufwerk U
- Vertrauliche Informationen
  - Personenbezogene Daten sind Angaben über eine bestimmte oder eine bestimmbare Person
    - Daten von Mitarbeiter
    - Daten zu Ansprechpartnern auf Kundenseite
  - Firmenbezogene Daten
    - Details zu Verträgen und Geschäftsbeziehungen
- Streng vertraulich
  - *z.B. Sourcecode, CAD-Zeichnungen, Verträge, Finanzdaten*

Schutzmaßnahmen

Organisatorische Maßnahmen

Technologische Maßnahmen

Physische Maßnahmen

Personenbezogene Maßnahmen

Organisatorische und technologische Maßnahmen

Zugriffsrechte und Passwörter

- Einschränkung de Zugriffsrechte
    - Festlegen von Rechtegruppen
    - Keine Admin-Rechte auf bereitgestellter Hardware
- Passwörtern
    - Für jede Anwendung individuelle Passwörter
    - Passwörter regelmäßig ändern

    - Keine Gruppenaccounts verwenden – Ausnahmen müssen mit der IT und dem ISB besprochen werden
    - Keine Weitergabe von Passwörtern an andere Mitarbeiter

Organisatorische und technologische Maßnahmen

Internetnutzung

- Bei der Internetnutzung auf einem Firmengerät gilt
    - Vorkonfigurierte Browser dürfen nicht verändert werden
    - Nutzung nur für berufliche Zwecke (außer in den Pausen)
    - GBS behält es sich vor, nicht angemessene Inhalte und Webseiten zentral zu sperren
    - Der Internetverkehr wird im Hintergrund protokolliert und kann bei begründeten Verdachtsfällen ausgewertet werden (SSL Scanning)

Organisatorische und technologische Maßnahmen

Data Loss Prevention

- Verhinderung von Datenabfluss (Data Loss Prevention (DLB))
    - Mechanismus, der automatisch bei jedem Speichern Versionen des Dokuments anlegt. (Bisher ohne Einschränkungen)
    - Löschen von Unterordnern nicht möglich (Unabsichtliches Löschen eines Ordners mit vielen Unterordnern)

Organisatorische und technologische Maßnahmen

Conditional Access

- Einschränkung des Zugriffs auf Firmendaten
    - Zugriff nur von registrierten Geräten (Notebooks, Handys, Tablets, etc.)
    - Zugriff nur aus DE, AT, CH, FR und NL
    - Regeln wurden von der IT und dem ISB erarbeitet und mit der Geschäftsleitung abgestimmt
    - Ausnahmen müssen bei der IT rechtzeitig beantragt und vom Vorgesetzen und dem ISB genehmigt werden
    - Registrierung privater Geräte in Ausnahmefällen nach Rücksprache möglich

Organisatorische und technologische Maßnahmen

Multifaktor Authentifizierung

- Anmeldung mit 2-Faktor-Authenifizierung
    - Wiederholte Abfragen
    - Dient der Authentifizierung des Benutzers

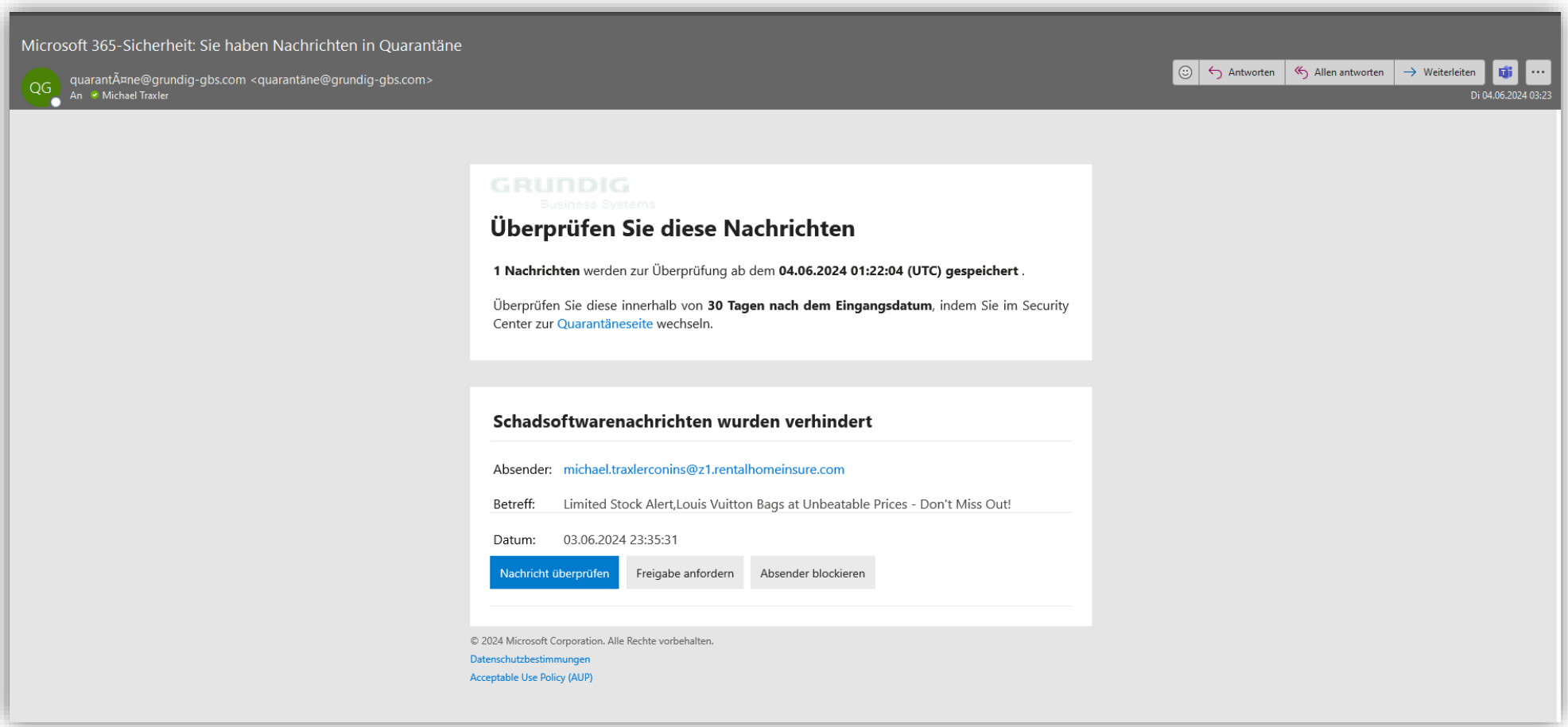
Personenbezogene Maßnahmen

Arbeitsplatzorganisation

- Sichtschutz für Bildschirme
    - Ab einem bestimmten Winkel kann der Bildschirm nicht mehr eingesehen werden
- Ausdrucke umgehend aus dem Drucker entfernen
- Beim Verlassen des Arbeitsplatzes Rechner sperren (WIN + L)
- Clean Desk
    - Keine Unterlagen nach Feierabend offen auf dem Tisch liegen lassen
    - Büros - wenn möglich - abschließen
    - Keine sensiblen Daten (z.B. personenbezogen) offen liegen lassen

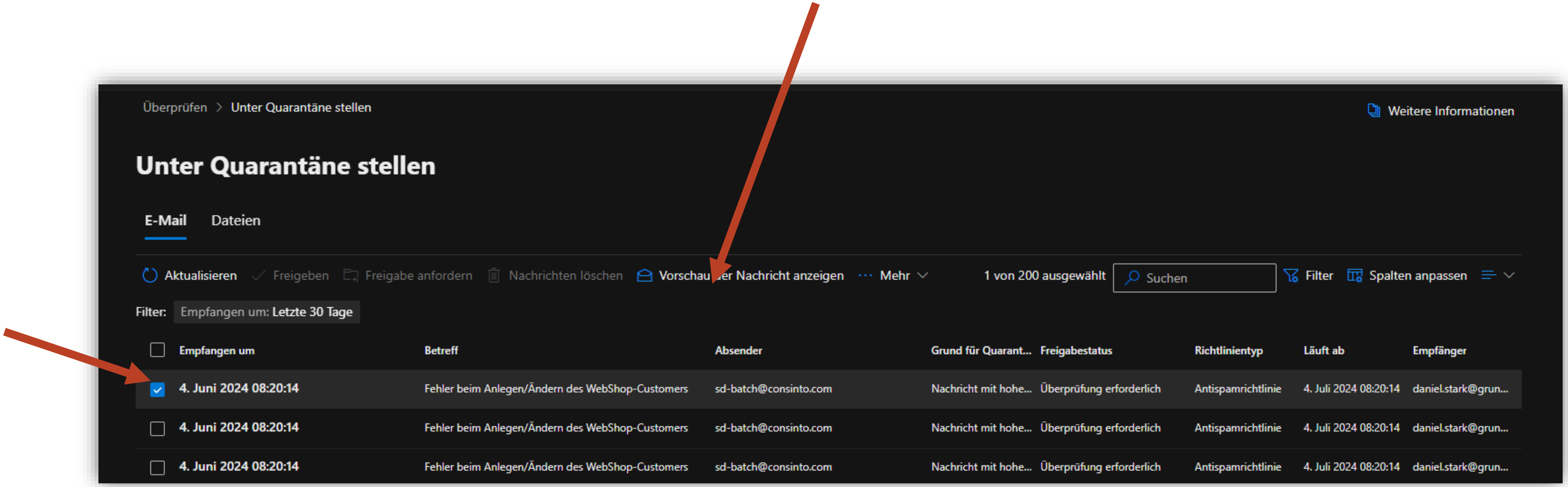
Personenbezogene Maßnahmen

Nachrichten überprüfen



Personenbezogene Maßnahmen

Nachrichten überprüfen 2



Personenbezogene Maßnahmen

Phishing-Mails erkennen

PHISHING-MAILS. Jeder einzelne Bestandteil einer verdächtigen E-Mail kann Ihnen Anhaltspunkte geben. Am besten, indem Sie sich Kontrollfragen stellen.

Zu «Von:»

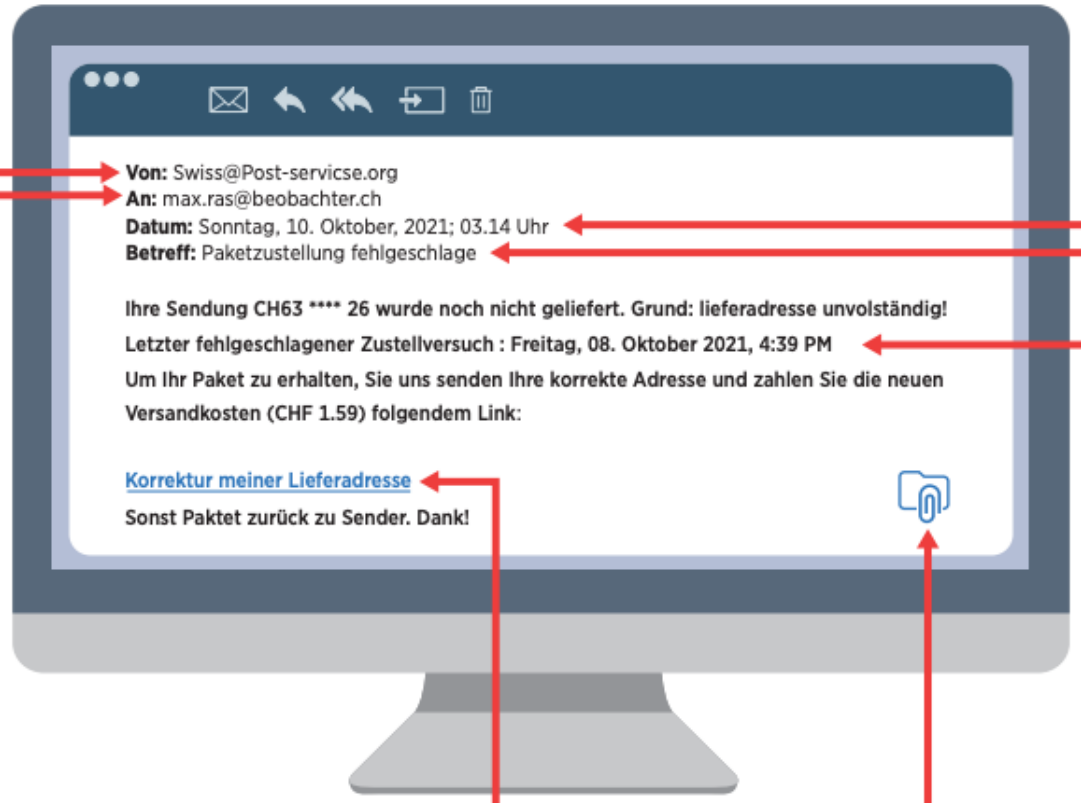
- Kennen Sie den Absender?
- Haben Sie mit diesem Absender üblicherweise Kontakt via Mail?
- Ist das überhaupt seine E-Mail-Adresse? (Der angezeigte Name kann täuschen. Wenn Sie mit dem Cursor über die Adresse des Absenders fahren, wird in manchen Mailprogrammen die hinterlegte E-Mail-Adresse angezeigt.)
- Bei vermeintlich offiziellen Absendern: Ist die E-Mail-Adresse plausibel?

Zu «An:» und «Cc:»

- Kennen Sie die anderen Empfänger/-innen? (Auch jene im Cc?)
- Ist die Zusammensetzung der Empfängerliste ungewöhnlich oder unplausibel?
- Gibt es andere Auffälligkeiten? (Zum Beispiel: Alle Empfänger/-innen beginnen mit dem gleichen Buchstaben)

Weitere Tipps

- Reagieren Sie nicht auf offensichtlichen Spam. Sonst wissen die Betrüger, dass Sie die Mail erhalten und angeschaut haben.
- Klicken Sie bei Spam auch nicht auf Unsubscribe-Links, damit bestätigen Sie nur Ihre E-Mail-Adresse.
- Für besonders starken Schutz deaktivieren Sie



Zu Links

- Versteckt sich hinter dem Link eine völlig

Zu Anhängen

- Klicken Sie in verdächtigen Mails nie auf

Zu Datum und Uhrzeit

- Ist der Zeitpunkt des Eintreffens bei diesem Absender plausibel? (In der Regel ist etwa sonntags oder nachts keine geschäftliche Korrespondenz zu erwarten.)

Zu «Betreff:»

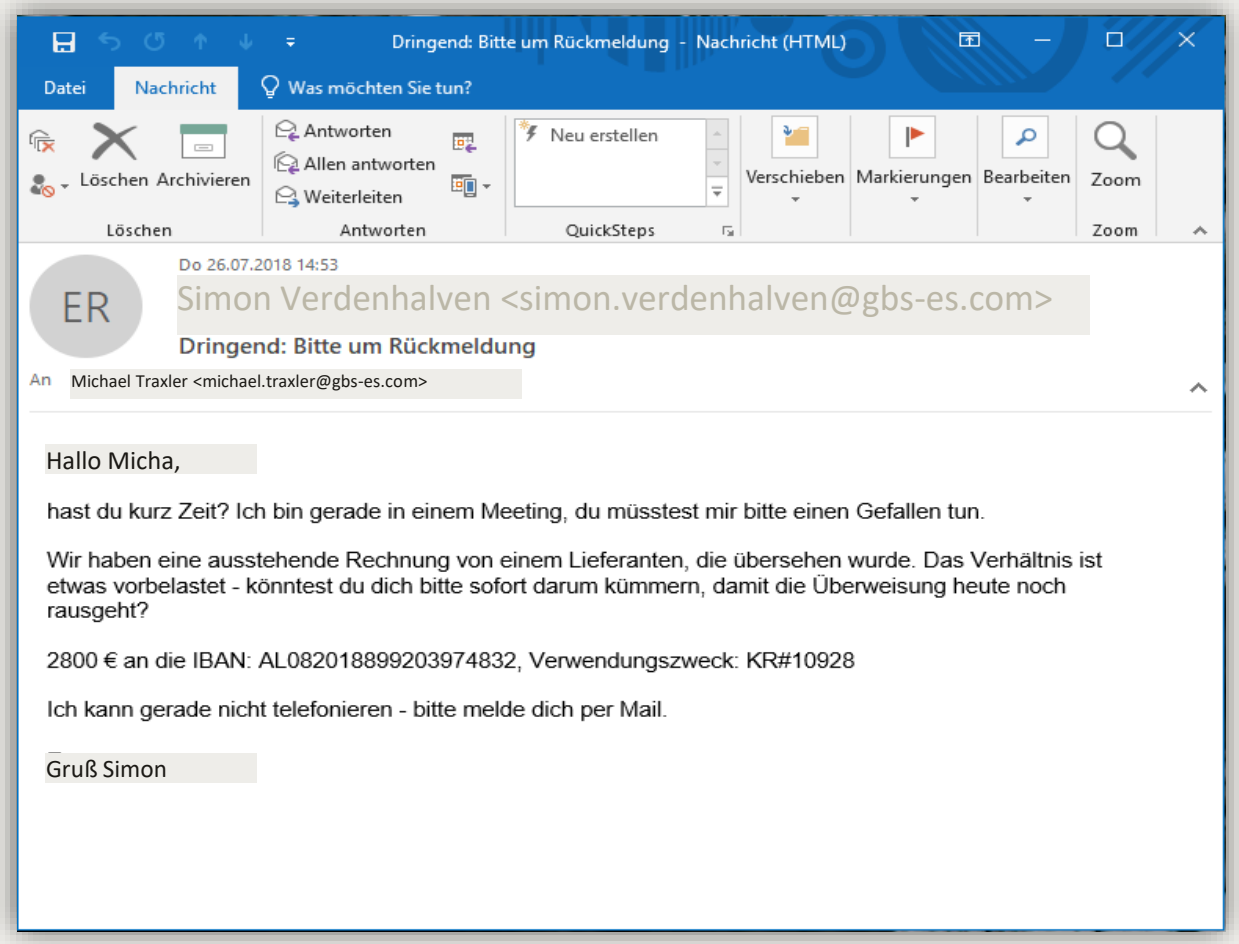
- Macht die Betreffzeile klar, worum es in der Mail geht, oder bleibt sie vage?
- Betrifft Sie der beschriebene Sachverhalt/das Thema wirklich?
- Gibt die Betreffzeile vor, eine Antwort auf eine E-Mail oder eine Anfrage zu sein («RE:» im Betreff), die Sie nie versandt haben?
- Ist dieses Thema für Sie relevant?
- Passen Betreffzeile und Inhalt zusammen?

Zum Inhalt

- Weist der Text ungewohnt viele Schreibfehler oder schlechte Grammatik auf, die auf ein Übersetzungsprogramm hinweisen könnten?
- Enthält die E-Mail lediglich einen Link oder eine Datei?
- Ist die Nachricht wirklich an Sie gerichtet, oder klingt sie eher allgemein?

Personenbezogene Maßnahmen

CEO Fraud erkennen



- Kein Vier-Augen-Prinzip
- Warum geht das nicht über die Buchhaltung?
- Wieso kein Lieferantenname?
- Wann fragt mich der Chef schon, etwas zu überweisen?
- Kurz innehalten und nachdenken: Ist das normal ?

GRUNDIG Business Systems

Melden

Was tun, wenn es passiert ist?

- Sofort Netzverbindungen trennen
  - Netzwerkkabel trennen
  - WLAN ausschalten
  - WLAN-Hotspot ausschalten
- PC herunterfahren
- IT informieren
  - Nicht über das infizierte Gerät!!
- Die letzten Schritte/Aktionen notieren, auch wenn es „peinlich“ ist.

Helpdesk:


it.support@grundig-gbs.com

0911-4758-220

GBS AUDIO

GRUNDIG Business Systems

Fragen?

GRUNDIG
Business Systems