Realschule ravensburg

E-Mail: info@realschule-ravensburg.de
Homepage: www.realschule-ravensburg.de
Wilhelmstraße 5-7
88212 Ravensburg
Telefon: (0751) 35 93 08-0
Telefax: (0751) 35 93 08-28

Ravensburg, 15.10.2022

Weitere Verbesserung der Datensicherheit an der Realschule Ravensburg

Liebe Eltern,

nach der aktuellen Einschätzung des BSI (Bundesamt für Sicherheit in der Informationstechnik) besteht hinsichtlich auch im Bereich Cybersecurity nach wie vor „eine erhöhte Bedrohungslage im Kontext des Krieges in der Ukraine“. Weitere Informationen finden sie unter diesem Link: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Ukraine-Krise/ukraine-krise_node.html

Unsere bisherigen Maßnahmen bescheinigen uns bereits einen guten Sicherheitslevel, der auf dem Niveau von Industrieunternehmen mit bis zu 1000 Mitarbeitern liegt.

Wir möchten uns weiter verbessern und unsere Schülerinnen und Schüler, sowie unsere Lehrkräfte bestmöglich schützen.

Aus diesem Grund werden wir folgende Maßnahmen umsetzen, bzw. haben bereits mit der Umsetzung begonnen:

- Aktivierung einer automatisierten Risikobewertung, um proaktiv Verbesserungsmaßnahmen vornehmen zu können (bereits umgesetzt).
- Regelmäßige Analysen und Verbesserung des Systems durch unser Systemhaus.
- Sperrung der Zugriffsmöglichkeiten aus dem Ausland (ebenfalls bereits aktiviert).
- Definition einer Passwortrichtlinie für sichere Passwörter
- Zwingende Verwendung der 2-Faktor-Authentifizierung
  (Die 2-Faktor-Authentifizierung bietet während der Anmeldung eine zusätzliche Schutzebene, bei der ein zweiter Identitätsnachweis z.B. durch eine SMS, ein Telefonanruf oder eine Authentifizierungs-App erbracht werden muss).
  Dadurch können wir künftig einen „Self service password reset“ anbieten, d.h. die Möglichkeit, ein vergessenes Passwort selbständig zurückzusetzen.

Was sind unsere nächsten Schritte?

1. Umsetzung der Maßnahmen bei unseren Lehrkräften als erste Pilotgruppe (bereits erfolgt)
2. Umsetzung der Maßnahmen und Sammeln von Feedback durch eine ausgewählte Pilot-Schülergruppe (bereits gestartet)
3. Umsetzung der Maßnahmen bei allen Schülerinnen und Schülern, **beginnend in diesem Monat**:
   a) Die Passwörter der Schülerinnen und Schüler werden zurückgesetzt.
   Damit stellen wir sicher, dass die Passwortänderung zeitnah erfolgt.
   b) Jedes Kind erhält ein Initialpasswort (d.h. ein erstes Passwort, um das persönliche neue Passwort eingeben zu können).
   c) Bei der ersten Anmeldung muss dann das Passwort geändert werden (Anforderungen an das neue Passwort siehe Anhang „Hinweise zur technischen Umsetzung“)
   d) Zeitgleich erfolgt die Einrichtung der 2-Faktor-Authentifizierung
   Mögliche Methoden sind:
      - SMS auf ein Mobiltelefon
      - Anruf zu einem beliebigen Telefonanschluss (Festnetz oder Handy)
      - Microsoft Authenticator App (unsere Empfehlung)

Bitte klären Sie mit Ihrem Kind **noch diese Woche, auf welche Art die Authentifizierung** stattfinden soll und laden Sie ggf. noch diese Woche die kostenlose App herunter.

(Hinweise zur App siehe „Hinweise zur technischen Umsetzung“)
Eine ausführliche Anleitung zur Einrichtung der 2-Faktor-Authentifizierung und für das neue Passwort erhält Ihr Kind auf unserer Homepage.

   e) Unterstützung bei der Umsetzung durch unsere IT-Lehrkräfte

      - in den Klassen 5 – 7 innerhalb der Schule
      - in den Klassen 8 – 10 wenn möglich in der Schule oder alternativ zuhause

Damit die Einrichtung der Security-Maßnahmen in der Schule mit Unterstützung der Lehrkräfte gelingen kann, ist es notwendig, dass Ihr Kind **am Tag der Einrichtung der Security-Maßnahmen sein Handy oder Tablet in die Schule mitbringt**.

Wir hoffen auf Ihre tatkräftige Unterstützung bei der Umsetzung der geplanten Maßnahmen.

Bei Problemen und Fragen steht Ihnen unsere IT-Lehrerin, Frau Bohner, nach den Herbstferien an folgenden Tagen zwischen 10:00 und 11:00 Uhr telefonisch unter 0751/359308-19 zur Verfügung:
jeweils mittwochs: 09.11.2022 / 16.11.2022 / 23.11.2022 / 01.12.2022

Mit freundlichen Grüßen

Michaela Steinhilber
Schulleiterin

Julian Leitner
stv. Schulleiter

Andrea Balle
stv. Schulleiterin

Hinweise zur technischen Umsetzung

Anforderung für das persönliche Passwort:

mindestens 14 Zeichen Länge

- Verwendung der Kombinationen aus
  - Großbuchstaben
  - Kleinbuchstaben
  - Ziffern
  - Sonderzeichen

- Wechsel des Passwords mindestens 1x pro Jahr

Einrichten der 2-Faktor-Authentifizierung:

Falls Sie sich für die kostenlose Authenticator App entschieden haben, dann können Sie diese herunterladen unter:

Aus dem Apple App Store	Aus dem Google play store
https://apps.apple.com/de/app/microsoft-authenticator/id983156458	https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=de&gl=US
App Store	Google Play

Eine schrittweise Anleitung zur Einrichtung der 2-Faktor-Authentifizierung und die Passwortänderung finden Sie auf unserer Homepage www.realschule-ravensburg.de

Hinweise zur Passwortsicherheit und zur Passwort-Verwaltung

- Zur Vereinfachung des Password handlings können Sie einen **kostenlosen Passwordmanager** (wie z.B. Enpass – in der Basislizenz kostenlos) verwenden. Damit können Sie komplexe Passwörter erstellen und verwalten.
- Verwenden Sie dieselben oder ähnliche Passwörter auf **keinen Fall mehrfach** für verschiedene Systeme!
- **Denken Sie auch immer an Ihre private Cybersicherheit.** Schützen Sie auch Ihre privaten Accounts durch komplexe Passwörter und 2-Faktor Authentifizierung, Auch hier hilft Ihnen ein Passwordmanager. Ein kompromittierter Account z.B. von Paypal oder Amazon kann Ihnen ggf. hohe Kosten verursachen. Diese Folgen können Sie auch im privaten Umfeld durch Anwendung unserer Hinweise nahezu ausschließen.

Bundesamt
für Sicherheit in der
Informationstechnik

BSI FÜR BÜRGER
INS INTERNET - MIT SICHERHEIT

Sichere Passwörter

BSI-Basistipp

Passwörter für den E-Mail-Account, Soziale Netzwerke oder den Computer sind wie Schlüssel für das eigene Zuhause: Nur ein sicheres Passwort schützt vor ungewollten Gästen und deren Zugriff auf persönliche Daten, Fotos oder Kontoinformationen.

Dabei gilt für den virtuellen Schlüssel, genauso wie für den Haustürschlüssel – je ausgefeilter, umso schwieriger ist es, das Schloss zu knacken.

Weitere Informationen:
https://www.bsi-fuer-buerger.de/Passwoerter

Umgang mit Passwörtern

- ☑ Passwörter unter Verschluss halten; Passwort-Manager sind eine gute Hilfe
- ☑ Passwörter spätestens bei Verdacht auf Missbrauch ändern
- ☑ Keine einheitlichen Passwörter für Accounts verwenden
- ☑ Voreingestellte Passwörter ändern
- ☑ Passwörter nicht an Dritte weitergeben und nicht per E-Mail versenden

Ein gutes Passwort ...

AleiPm4Z+eK!*

- ... sollte mindestens acht Zeichen lang sein, je länger desto besser.
- ... besteht nicht aus einer Kombination mit Geburtstagen oder Namen des Haustieres.
- ... sollte nicht im Wörterbuch stehen.
- ... darf keine gängigen Wiederholungs- oder Tastaturmuster (asdfgh oder 1234abcd) enthalten.
- ... ist kein simples Passwort, das einfach um ein Sonderzeichen am Anfang oder Ende ergänzt wird.
- ... kann aus Groß- und Kleinbuchstaben, Sonderzeichen (?!%+) und Ziffern bestehen.

Bei Reisen ins Ausland können Umlaute auf landestypischen Tastaturen evtl. nicht eingegeben werden.

*) Die Eselsbrücke: Indem Sie sich jeweils den ersten Buchstaben eines jeden Wortes in einem Satz merken, können Sie sich ganz einfach an ein Passwort mit mehr als acht Zeichen erinnern. Schon sind Sie bestens geschützt. Beispiel: „Am liebsten esse ich Pizza mit vier Zutaten und extra Käse!" wird zum Passwort: AleiPm4Z+eK!