# Stadt Bielefeld

## IT-Newsletter

### Sonderausgabe Datensicherheit insbesondere im städtischen Datennetz

www.bielefeld.de

April 2024

## Sehr geehrte Schulleitungen, sehr geehrte Lehrkräfte und Medienbeauftragte,


**IT-Hotline**
**Amt für Schule**
**☎ 0521 51-2700**
**it.schulen@bielefeld.de**

„Ab dem 6. Juli 2021 geht in der Landkreisverwaltung von Anhalt-Bitterfeld nichts mehr. Hacker haben Daten verschlüsselt und erpressen den Landkreis. "You are fucked" ist ihre erste Nachricht."

*Quelle: Podcast in der ARD Audiothek*

„In der Nacht auf den 30.10.2023 wurde bei der Südwestfalen-IT (SIT) ein Ransomware-Angriff entdeckt. Die SIT ist ein [...] IT-Dienstleister für 72 Kommunen – darunter alle Kommunen in Südwestfalen [...]. Deshalb waren neben der SIT selbst all diese Kommunen von dem Angriff betroffen, sprich, sie konnten ihre IT nicht mehr nutzen und auch digitale Dienstleistungen für die Bürger:innen nicht mehr anbieten. Nach Informationen vom 31.10. ist damit die IT oder große Teile davon in 72 Kommunen mit 22.000 Arbeitsplätzen ausgefallen [...] sowie mehrere Kommunen im Rheinisch-Bergischen Kreis und einige kommunale Unternehmen."

*Quelle: Eintrag im KommunalWiki der Heinrich-Böll-Stiftung | Artikel auf welt.de*

Wie Sie erkennen, wird das Thema Datensicherheit immer wichtiger. Es geht dabei nicht nur darum Ihre eigenen Daten, sondern auch um das große Ganze wie das Verwaltungsnetz und das pädagogische Netz zu schützen.

Seit geraumer Zeit werden sowohl das gesamte städtische Netz als auch einzelne städtische Schulen von außen angegriffen. Vieles lässt sich technisch abfangen und wir arbeiten stetig an der Verbesserung des Schutzes. Jedoch können alle Nutzer des Verwaltungsnetzes aktiv durch ein wenig Misstrauen und den gesunden Menschenverstand einen großen Beitrag zur Sicherheit leisten. Ebenso gilt dies innerhalb des pädagogischen Netzes.

Sie arbeiten täglich mit städtischen Geräten sowie Programmen und haben Zugang zum städtischen Netz (Verwaltungsnetz). Daher möchten wir Sie mit den nachfolgenden Punkten für den sicheren Umgang mit den Geräten, den Programmen sowie dem Datennetz sensibilisieren. Die genannten Punkte sind auch für das pädagogische Netz sinnvoll und übertragbar.

*Mit freundlichen Grüßen*
*Ihr IT-Team des Amtes für Schule*

## Bereitstellung und Nutzung von Hard- und Software

Grundsätzlich darf innerhalb des Verwaltungsnetz lediglich die von der Stadt Bielefeld und/oder dem Amt für Schule bereitgestellte Hard- und Software zum Einsatz kommen. Über die Standardausstattung hinaus benötigte Hardware kann in Abstimmung mit dem Amt für Schule (400.231) bestellt und verwendet werden.

Benötigen Sie weitere Software für die Erledigung Ihrer Aufgaben, so teilen Sie dies dem Amt für Schule mit. Unterlassen Sie es Tools und Software aus dem Internet zu laden oder über einen USB-Stick auf den Rechner zu bringen und dort auszuführen.

Private oder USB-Sticks unbekannter Herkunft sind auf keinen Fall zu verwenden. Die Verwendung von USB-Sticks zur Datenübertragung sollte gar nicht stattfinden. Hierzu sind Netzlaufwerke effektiver und sicherer. Ist im begründeten Einzelfall ein USB-Stick notwendig, fordern Sie diesen über das Amt für Schule an. Diese Sticks werden am Verwaltungsrechner nur verschlüsselt genutzt.

Derzeit verwendete Hardware, die nicht durch die Stadt bereitgestellt wird, wie Multifunktionsgeräte oder Drucker, werden sukzessive durch das Amt für Schule ausgetauscht.

Die Nutzung privater Geräte im städtischen Netz ist grundsätzlich untersagt. Gleiches gilt für die Daten: Keine privaten Daten auf beruflichen Geräten!

Wird durch die städtische IT-Abteilung ein befallener oder kompromittierter Rechner im Verwaltungsnetz festgestellt, so wird dieser sofort gesperrt und auf Werkseinstellungen zurückgesetzt! Der Rechner ist für Sie dann nicht mehr nutzbar und alle nicht auf Netzlaufwerken gesicherten Daten sind dann unwiederbringlich gelöscht.

### Protokollierung

Im Verwaltungsnetz werden Systemaktivitäten wie Anmeldung, Abmeldung, Datenzugriffe sowie Internetzugriffe protokolliert und innerhalb der vorgegebenen Frist gespeichert. Diese Daten werden nicht zum Zwecke der Leistungskontrolle herangezogen. Begründet durch Sicherheitsvorfälle wird anlassbezogen die Aktivität betroffener Geräte und der beteiligten Nutzer ausgewertet. Sollten dabei personenbezogenen Daten berührt sein, wird der städtische sowie schulische Datenschutzbeauftragte beteiligt.

### Arbeiten mit personenbezogenen Daten

Bei der Arbeit mit personenbezogenen Daten, wie in der Schulverwaltungssoftware, ist sicherzustellen, dass unbefugte Dritte den Bildschirm nicht einsehen können. Dies kann beispielsweise durch die Ausrichtung des Monitors im Sekretariat mit Publikumsverkehr sichergestellt werden.

Der Computer ist bei jedem, auch kurzzeitigen, Verlassen des Arbeitsplatzes zu sperren. Hierzu nutzen Sie das Tastenkürzel „Windows-Taste + L“. Dadurch ist der Zugang durch Dritte verhindert.

### Zugriffsrechte und Berechtigungen

Zugriffe auf die Ordnerstrukturen der Netzlaufwerke X und Z werden durch Berechtigungen geregelt. Fehlende Berechtigungen oder Änderungen werden durch das Amt für Schule ergänzt bzw. angepasst. Bitte teilen Sie uns mit, wenn sich Aufgaben ändern und dadurch ein Zugang, beispielsweise zu SchILD, nicht mehr benötigt wird oder angepasst werden muss (Schulwechsel). Nur so lässt sich die Datensicherheit mithilfe der notwendigen Berechtigungen sicherstellen!

### Datensicherung

Alle auf den zentralen Laufwerken X und Y gespeicherten Daten unterliegen einer automatischen Sicherung und sind bei Bedarf bis zu drei Monate rückwirkend wiederherstellbar, Einzeldateien ggf. kürzer.

Persönliche Daten sollen auf dem X-Laufwerk im Ordner X:\Benutzer\BI-Schlüssel_bzw._X-Schlüssel gespeichert werden. Dann sind diese ebenfalls in der automatischen Sicherung enthalten. Auf dem Rechner selber werden keine Daten automatisch gesichert.

## Passwörter

Passwörter für Windows oder Softwareanwendungen sind individuell festzulegen. Passwörter sollten komplex sein. Einfache Passwörter wie „12345" oder der eigene Name sowie Initialkennwörter (auch mit kleineren Abwandlungen) sind nicht sicher genug.

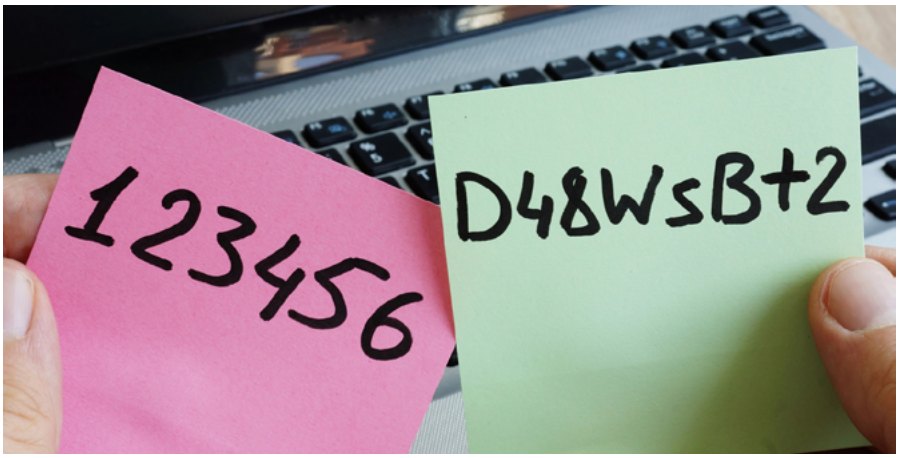
Die Eingabe des Passwortes muss unbeobachtet erfolgen. Geben Sie ein persönliches Passwort nicht weiter, auch um sich selber vor Missbrauch durch Dritte zu schützen! Sollten mehrere Personen auf ein und dieselbe Ressource Zugriff benötigen, sprechen Sie mit uns über Möglichkeiten. Passwörter werden auch nicht unverschlüsselt abgespeichert/abgelegt. Das Aufschreiben eines Passwortes auf einen Zettel o.ä. und diesen bspw. an den Monitor kleben oder unter die Tastatur zu legen sind keine geeigneten „Merkstrategien" und zu unterlassen.

Für die Verwaltung von mehreren Passwörtern kann ein Passwortmanager wie „KeePass" verwendet werden. Dieser ist auf Verwaltungsarbeitsplätzen bereits installiert. Zur Unterstützung der Einrichtung wenden Sie sich das Amt für Schule oder die 1333.

Mögliche Merkstrategie: Das Passwort entsteht aus einem Satz, von dem jeder Anfangsbuchstabe und jedes Zeichen übernommen wird: „Am liebsten esse ich Pizza mit 4 Zutaten!" = „AleiPm4Z!".

Allgemein empfehlen wir, wählen Sie ein Passwort, das Sie sich gut merken können. Dabei sollte auch die Länge des Passwortes bedacht werden, mindestens acht Zeichen lang, je länger und komplexer desto besser. Verwenden Sie unterschiedliche Buchstaben, Groß- und Kleinschreibung, Sonderzeichen, Umlaute und Ziffern.

*Weitere Informationen: Empfehlungen Bundesamt für Sicherheit in der Informationstechnik für sicheres Passwort*




## Verschlüsselte Datenübermittlung

E-Mails mit vertraulichen oder personenbezogenen Daten dürfen nur verschlüsselt versendet werden. E-Mails innerhalb der Domain „bielefeld.de", also Sender und Empfänger nutzen eine E-Mail-Adresse innerhalb „...@bielefeld.de", werden innerhalb eines vertrauenswürdigen Systems übertragen.

Verschlüsselt werden alle Mails von/an Behörden, soweit diese an das Netz des Bundes (NdB, früher DOI) angebunden sind, wie bspw. Landesbehörden oder andere Schulträger. E-Mails, die Sie auf diesem Weg erreichen, sind in der Betreffzeile mit „via DOI" gekennzeichnet.

Ist es Ihrerseits erforderlich/gewünscht, dass schützenswerte Daten verschlüsselt übermittelt werden, so ist hierzu das Amt für Schule einzubeziehen.

## E-Mail-Adressen

Die bereitgestellte E-Mail-Adresse, typischer Weise vorname.nachname@bielefeld.de, ist lediglich zur Erfüllung der schulischen Aufgaben zu nutzen.

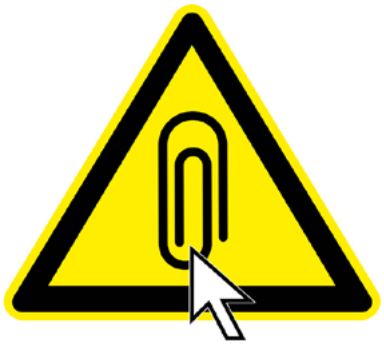
Legen Sie in Outlook Vertretungen/Stellvertretungen fest, damit diese im Falle von Abwesenheit auch Ihre E-Mails bearbeiten dürfen und können. Weiter hinterlegen Sie in Outlook für ausgehenden Mails eine Signatur. Diese sollte mindestens Name, Schulname, Anschrift sowie Ihre oder allgemeine Kontaktdaten wie Telefon, E-Mail und ggf. Fax enthalten.

## Links und Anhänge

Klicken Sie nicht auf Internet-Links in Mails oder Dokumenten deren Herkunft Sie nicht sicher kennen. Oft sehen Mails mit böswilligen Links (wie Phishing) auf den ersten Blick aus wie Mails von bekannten Personen, Firmen oder Organisationen.

Öffnen Sie nicht leichtfertig Anhänge aus eingegangenen Mails. Auch selbst von bekannten Mail-Adressen können bösartige Anhänge verschickt werden, wenn dessen Rechner kompromittiert ist. Im Zweifel öffnen Sie die Links und Anhänge nicht und wenden sich an das Amt für Schule oder die 1333!

Werden Sie beim Öffnen von per E-Mail zugesandten Office-Anhängen wie Word, Excel oder PowerPoint aufgefordert „Inhalte zu aktivieren": Lehnen Sie das ab! Sie



können das Dokument auch ohne aktivierte Makros lesen.

Wenn Sie Zweifel haben, ob ein Link oder ein Anhang schädlich ist, können Sie die IT-Hotline um Unterstützung bitten. Senden Sie dann bitte die betroffene E-Mail als Anhang an it-service@stadtwerke-bielefeld.de. Bitte verwenden Sie nicht die Funktion „Weiterleiten", da dadurch relevante und für die Einschätzung wichtige Informationen aus den E-Mail-Headern verloren gehen.

Nachfolgend ein paar einfache Beispiele, wie Sie Mails mit böswilligen Links oder Anhängen erkennen können: Fehlen in eingehenden E-Mails elementare Inhalte wie Begrüßung oder ein Grußwort, sind die Mails auffällig kurzgehalten, sind für den vermeintlichen Absender untypisch viele Rechtschreibfehler enthalten oder liegt ein ungewöhnlicher Satzbau vor, so kann es sich um eine Mail mit böswilligen Link oder Anhang handeln. Bin ich mir unsicher, lieber einmal weniger klicken! Bei Zweifeln über den Charakter einer E-Mail kontaktieren Sie die Hotline 1333 oder das Amt für Schule. Nur hier erhalten Sie eine aussagekräftige Antwort.

Fällt Ihnen eine E-Mail als eindeutig unerwünscht (SPAM) auf, dann senden Sie diese E-Mail als Anhang an Postkasten_Spam (Spam@stadtwerke-bielefeld.de). Mit den dort eingehenden Mails werden die Erkennungsfilter nachjustiert. Damit sollten Sie die SPAM nach einiger Zeit nicht mehr erhalten.

## Kontakt und Supportpartner

**Bei Fragen oder Problemen zu oder mit städtischer Hardware und städtischer sowie schulspezifischer Software auf dem Verwaltungsrechner ist vorrangig der Support des Amts für Schule (400.231) einzubeziehen. Erreichbar per E-Mail it.schulen@bielefeld.de oder per Telefon 0521 51-2700**

**Netzstörungen oder Ausfälle von Verwaltungsarbeitsplätzen oder Telefonie sowie Sicherheitsvorfälle melden Sie dem zentralen IT-Service der Stadt per E-Mail it-service@stadtwerke-bielefeld.de oder über die IT-Hotline 0521 51-1333.**

**Bei Fragen oder Problemen zu oder mit Hard- oder Software im pädagogischen Netz ist die erste Ansprechperson der Schul-IT-Manager Ihrer Schule.**

**Bitte teilen Sie dies wichtigen Informationen mit Ihren Kolleginnen und Kollegen, die im städtischen Datennetz (Verwaltungsnetz) arbeiten!**

**Impressum**
**Herausgegeben von:**

Stadt Bielefeld
Amt für Schule

**Verantwortlich im Sinne des Presserechts:** Susanne Beckmann

**Redaktion:** Daniel Klösener, Amt für Schule

**Kontakt:**
E-Mail: Daniel.Kloesener@bielefeld.de
Tel.: 0521 51-3965

**Ausgabe:** Sonderausgabe 04/2024

**Gestaltung:** Druckservice, Stadt Bielefeld

**Bildnachweise:**
Titel: Podcast in der ARD Audiothek
Verschlüsselte Datenübermittlung: Panthermedia – maxkabakov
Passwort: Panthermedia – designer491
E-Mail: Stadt Bielefeld
Links und Anhänge: Panthermedia – Bambara (YAYMicro)