Sehr geehrte Schulleiterinnen und Schulleiter,

in den letzten Tagen erreichen uns Meldungen von Schulen, dass zurzeit verstärkt gefälschte Mails mit angehängten Word-Dokumenten oder mit gefährlichen Links in Ihren Postfächern landen. Oft erscheinen die Absender als bekannt und die Ansprache vertraut, da diese sich auf eine bekannte Konversation zu beziehen scheint. So sollen Sie neugierig gemacht und in Sicherheit gewogen werden, um jegliche Skepsis erst gar nicht aufkommen zu lassen.

Bei den Anhängen handelt es sich um Dateien im alten Word-Format mit der Endung ".doc". Es kann allerdings nicht ausgeschlossen werden, dass auch andere Datei-Formate genutzt werden, um auf Ihrem PC oder gar im gesamten Netzwerk Schadsoftware zu installieren. Auch Endungen von Bilddateien wie ".jpg", ".png", ".zip"-Dateien oder auch andere Office-Dateien wie ".docm", ".xls/.xlsm", ".ppt/.pptm" können vorkommen.

Beim Öffnen dieser Dateien gibt es mehrere mögliche Szenarien, welche Ihre Arbeit stark beeinträchtigen können:

- Es wird - unbemerkt durch den Empfänger der Mail - weitere schädliche Software aus dem Internet nachgeladen, die z.B. die Dateien Ihres Computers, Ihrer Backups und vielleicht sogar des gesamten Netzes verschlüsseln. Eine Wiederherstellung ist kaum mehr möglich.
- Ihre Adressbücher, Nutzernamen und Passwörter sowie die Mailkommunikation werden abgegriffen und an unbekannte Dritte verschickt.
- Der Datenverkehr zwischen Ihnen und anderen könnte unbemerkt kontrolliert werden.
- Ihre Computer bzw. Ihre Zugänge werden für Attacken auf weitere Rechner und Geräte im Internet genutzt.
- Ihre Reputation und die des Landes Berlins leiden so stark, dass Mails mit der Endung "schule.berlin.de" nicht mehr zugestellt werden können.
- Die Internetzugänge werden bis zur Behebung des Problems gesperrt.

Das Öffnen solcher Mailanhänge muss keine unmittelbare Ausführung des Schadcodes nach sich ziehen, denn manchmal agiert diese Software auch zeitverzögert und unbemerkt. Dies sollte also nicht ignoriert und daher unverzüglich an das Schulservicezentrum Berlin (SSZB) gemeldet werden. Sollte dennoch einmal ein solcher Anhang im Verwaltungsnetz geöffnet worden sein, so informieren Sie bitte umgehend das Schulservicezentrum Berlin unter der Telefonnummer 030 - 9021 4666. Es werden die weiteren Maßnahmen mit Ihnen besprochen.

Bitte weisen Sie alle Ihre Mitarbeiter auf diese Problematik hin, denn das Problem beschränkt sich nicht nur auf die Computer der Verwaltung. Halten Sie unbedingt telefonische Rücksprache mit dem Absender, wenn Ihnen eine Mail mit Anhang verdächtig vorkommen sollte. Gerne werden solche Mails auch als Bewerbungen direkt an die Schulen versendet. Wenn die Mail keine weiteren

Informationen mit einer Rückrufnummer enthält, die Sie dann auch verwenden sollten, löschen Sie die Mail lieber gleich. Ein ernsthafter Bewerber wird sich erneut melden, genauso wie ein Rechnungsersteller oder jemand, der Ihnen unbedingt etwas schenken möchte.

Sie selbst können eine Gefährdung anderer verringern, indem Sie nur noch das neuere ".docx"-Format Ihres Office-Programms statt des ".doc"-Formats zum Speichern verwenden.

Sie benötigen weitere Beratung zu Fragen rund um die Sicherheit Ihrer IT in der Schule? Dann können Sie unter dem Link https://www.egovschool-berlin.de/node/409 Ihre Regionalen Informationssicherheitsbeauftragten kontaktieren und einen Gesprächstermin vereinbaren.

Mit freundlichen Grüßen
Schulservicezentrum Berlin

-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --

Senatsverwaltung für Bildung, Jugend und Familie
Schulservicezentrum-Berlin
Alt-Friedrichsfelde 60 – 10315 Berlin
Telefon: +49 30 9021 4666
E-Mail: sszb@schule.berlin.de