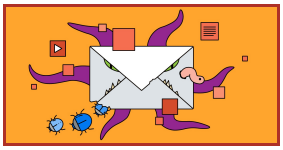
Dear all,

anbei findet ihr die aktuellsten IT-bezogenen News.

Wiederaufbau nach Cyberangriff

Am Freitag vor Pfingsten (29.05.2020) wurde die Universitäts- und Stadtbibliothek (USB) Ziel eines kurzfristig detektierten Cyberangriffs. Alle zentralen IT-Systeme wie Katalogrecherche, Buchausleihe, Nutzerkonten, Mailserver und Homepage wurden vom Netz getrennt und sind bis heute noch eingeschränkt verfügbar. Aktuelle Informationen zur Rekonstruktion der IT-Systeme erfahren Sie auf der folgenden Seite und auf der Homepage der USB.



E-Mails mit Anhängen, die Makros enthalten

Durch die zunehmende Bedrohung von Schadsoftware im Bereich des E-Mail-Verkehrs werden von der RRZK keine E-Mails in Form von Microsoft Office-Dokumenten mit Makros als Anhang von außerhalb der Uni angenommen. Eine derartige Schadsoftware kann Schäden sowohl auf dem lokalen Rechner als auch im gesamten Intranet der UzK verursachen.
Um weitere Einzelheiten zu erfahren könnt ihr folgende wichtige Informationen auf der RRZK Seite nachlesen.

Phishing / Spear-Phishing

Bei „Spear-Phishing“ handelt es sich um spezielle Betrugsversuche mit gefälschten E-Mails oder Kurznachrichten. Cyberkriminelle versuchen an die Daten des Benutzers zu kommen, diese für kriminelle Zwecke zu nutzen oder auch Malware auf dem angegriffenen Computer zu installieren und diesen zu kompromittieren. An dieser Stelle ist es auch wichtig, kurz den Unterschied zwischen Phishing und Spear-Phishing zu

erwähnen.
Bei Phishing Mails handelt es sich meist um unpersönliche Anreden wie z.B. „Sehr geehrter Kunde“ und ist an mehrere Hundert bis Tausende Personen gerichtet. Im Gegensatz dazu ist das Vorgehen bei Spear Phishing ein gut gezielter Angriff auf ein bestimmtes Opfer.
Weitere wichtige Beispiele und Vorsichtmaßnahmen können ebenso auf der RRZK-Seite gelesen werden.

Mit freundlichen Grüßen
Muzamal Cheema

Button

Impressum:
SFB Prominence in Language
Luxemburger Str. 299
50939 Köln