Bistum Essen

ERZBISTUM KÖLN

KATHOLISCHE KIRCHE
BISTUM MÜNSTER

Handlungsempfehlung für Authentifizierungsmaßnahmen bei Webzugängen

Arbeitsgruppe für Informationssicherheit der NRW Bistümer Version X0.3

Kirche im Bistum Aachen

Erzbistum Paderborn

ZIELGRUPPE

Diese Handlungsempfehlung richtet sich an Verantwortliche und Dienstleistende, welche eine sichere Authentifizierung für Anwendungen/Dienste im kirchlichen Umfeld umsetzen oder nutzen müssen.

EINLEITUNG

Als Verantwortliche und Dienstleistende für kirchliche und kirchennahe Services tragen Sie die Verantwortung nicht nur für Daten in Ihrem eigenen direkten Umfeld, sondern auch für die Ihrer Nutzer. Sollte auch nur ein Teil dieser sensiblen Daten und IT-Services inzwischen online erreichbar sein – sei es über Cloud Speicherdienste, Webanwendungen oder Webmailzugänge – enthalten all diese Systeme vertrauliche Informationen, die einem besonderen Schutz unterliegen.

Gerade kirchliche und insbesondere auch Personaldaten können dabei für Angreifende besonders interessant sein.

Daher sind zum einen die Kosten zu bedenken, die ein erfolgreicher Angriff mit sich bringen kann, aber auch der Reputationsverlust durch ein mögliches Bekanntwerden ist signifikant und langfristig spürbar.

Zwischen potenziellen Angreifenden und den sensiblen Daten steht in manchen Fällen leider bisher nur die Verwendung eines einzelnen Passwortes.

Wir als Arbeitsgruppe für Informationssicherheit der NRW-Bistümer möchten Ihnen im Folgenden kurz aufzeigen, wie Sie die Sicherheit für sich und Ihre Anwendungen verhältnismäßig einfach, aber dafür umso deutlicher erhöhen können:

WARUM EIN PASSWORT ALLEINE NICHT AUSREICHT

Die Nutzenden authentifizieren sich in der Regel mit einer Benutzerkennung und einem ersten Faktor wie beispielsweise einem Passwort. Anhand der Eingabe können die Nutzenden identifiziert werden und erhalten die ihnen zugeordneten Rechte am System. Wenn für bestimmte Daten oder Dienste ein besonderer Schutzbedarf identifiziert wurde, wurde in der Vergangenheit oft einfach die Komplexität oder Länge des Passworts vergrößert. Dies hat sich in der Praxis als wenig zielführend herausgestellt. Passwörter werden in der Folge immer länger und komplexer. Die Nutzenden neigen dann – verständlicherweise – zu Umgehungsstrategien (Aufschreiben, Musterbildung, Mehrfachnutzung).

Die (ausschließliche) Nutzung von Passwörtern hat also erhebliche Nachteile:

- Umgehung der Passwortkomplexität bei den Nutzenden (Angriffsmethode: Password-Spraying)
- Wiederverwendung der Passwörter durch die Nutzenden (Angriffsmethode: Password-Replay)
- Unzureichende Sicherheit beim Speichern von Passwörtern

Verschiedene Methoden, wie beispielsweise Phishing oder Brute Force Angriffe, sind geeignet Passwörter schnell zu erbeuten. In vielen Fällen müssen die Angreifendenden auch gar nicht das eigentliche Ziel attackieren. Häufig sind bereits öffentlich gewordene Kennwörter in Verbindung mit Konten anderer Services frei verfügbar im Internet zugänglich. Auch das Mitlesen von Passwörtern per Keylogger, besonders auf fremden beziehungsweise öffentlichen Rechnern, ist ein ernstzunehmendes Risiko.

Es ist zu beachten, dass kompromittierte Benutzerkonten häufig als erste Einstiegspunkte in eine Organisation genutzt werden, um zunächst erst einmal Informationen zu sammeln und erst später weitere Angriffe durchzuführen.

Um den Sicherheitsstandard signifikant zu erhöhen empfiehlt es sich den Passwortschutz durch eine zweite Barriere zu ergänzen: Die Multi-Faktor-Authentifizierung.

WAS IST DIE MULTI-FAKTOR-AUTHENTIFIZIERUNG (MFA)?

Mit der Multi-Faktor-Authentifizierung wird das Passwort allein in den Händen der Angreifendenden nutzlos, da hierbei die Anmeldung um einen physisch getrennten zweiten Kanal ergänzt und somit das Risiko eines erfolgreichen Angriffs gesenkt wird.

Für eine Anmeldung an einem Dienst werden zunächst Benutzername und Passwort eingegeben. Im Anschluss daran wird ein zweiter Faktor erforderlich, um den Login zu vervollständigen.

Konkret bedeutet dies, dass die Angreifendenden immer auch den zweiten Faktor benötigen, um auf das Konto zugreifen zu können. An diesen heranzukommen ist aber wesentlich schwieriger als ein Passwort zu erbeuten.

MÖGLICHKEITEN EINER MULTI-FAKTOR-AUTHENTIFIZIERUNG

Konkrete Umsetzungen für eine Zwei-Faktor-Authentifikation können wie folgt aussehen:

- Hardware-Sicherheitstoken: Der zweite Faktor wird über einen speziellen kryptografischen USB-Stick oder eine Chipkarte abgerufen.
- Software-Sicherheitstoken: Der zweite Faktor wird über ein Mobiltelefon als Code abgerufen
- Körpermerkmal: Erst das zusätzliche Einlesen eines Fingerabdrucks macht den Zugang zu dem System möglich.

Dabei sind beliebige Kombinationen aus Wissen, Besitz und/oder Körpermerkmal möglich.

UNSERE HANDLUNGSEMPFEHLUNG

Zunächst sollten Sie abschätzen, wie hoch das Risiko und die Folgen eines Angriffs in Abhängigkeit mit den gespeicherten oder zu verarbeiteten Daten sind. Dabei sollten mindestens die folgenden Fragestellungen Beachtung finden:

- Sind die Anwendungen oder Dienste extern erreichbar?
- Handelt es sich um kritische administrative Zugänge (intern/extern)?
- Sind sensible Informationen in den Diensten enthalten?
- Sind datenschutzrelevante Informationen in den Diensten enthalten?

Wird mindestens eine dieser Fragen mit ja beantwortet, sollten entsprechend für diesen Bereich sichere Authentifizierungsverfahren implementiert werden. Derzeit ist die Nutzung eines zweiten Faktors eine der effektivsten Methoden zur Sicherstellung der Identität und damit zur Wahrung der Vertraulichkeit schützenswerter Dienste und Daten.

Beispiele:

Extern erreichbare Dienste

- Veröffentlichte Webdienste (im Einzelfall auch nur die administrativen Zugänge)
- Chat/Video Anwendungen
- Speicherlösungen • Einwahl in interne Ressourcen (Virtual Desk, VPN etc.)
- Web-Mail

Kritische administrative Zugänge (intern/extern)

- Anwendungsadministratoren
- Infrastruktur Administratoren (Netzwerk, Server, Application und Appliance)
- Backup/Restore Administration

Anwendungen mit sensiblen oder datenschutzrelevanten Informationen

- Kirchliches Meldewesen
- Personal- und Finanzmanagement
- KitaPlus

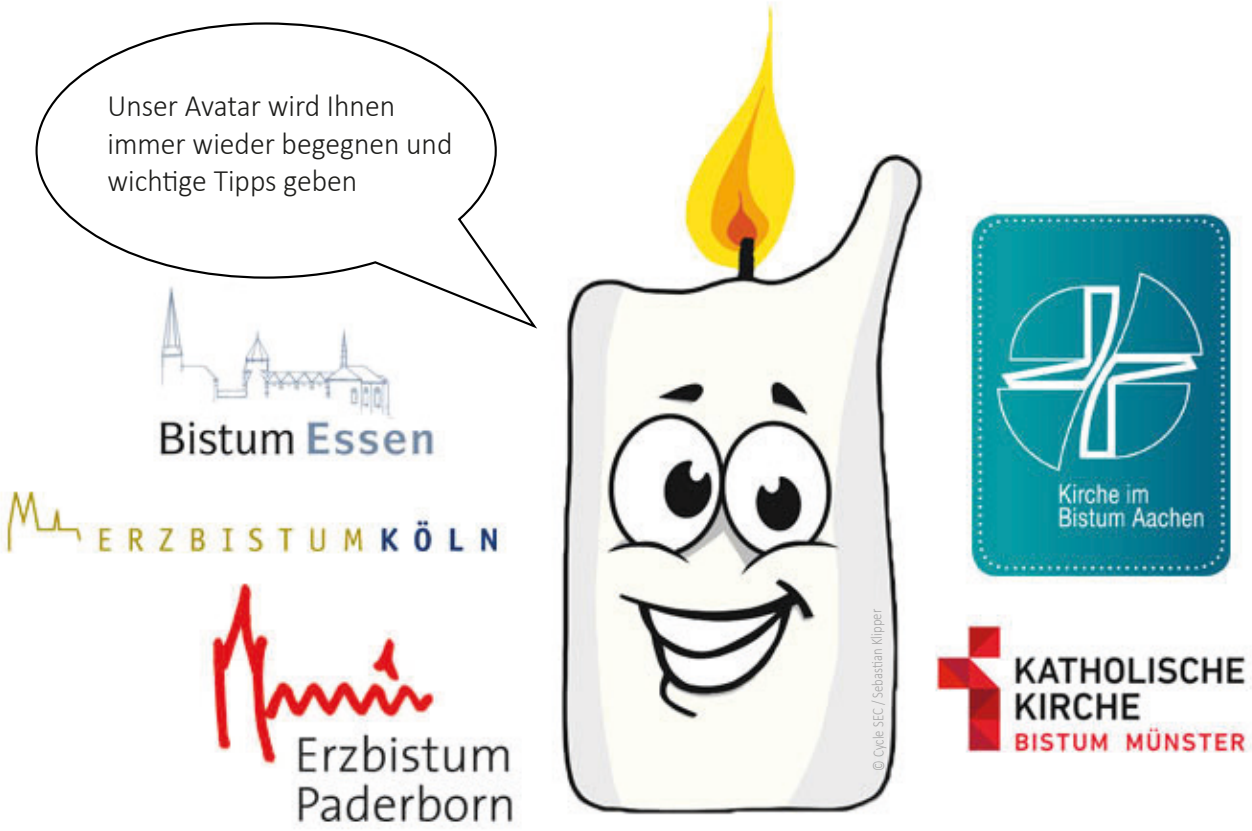
WEITERGEHENDE INFORMATIONEN

[Stand: 12/2020]

BSI: Zwei-Faktor-Authentisierung um die Komplexität des Passworts zu reduzieren:
www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

BSI: Zwei-Faktor-Authentisierung für höhere Sicherheit:
www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei-Faktor-Authentisierung_node.html;jsessionid=7229D801C72ED339861288B3FCF4AB5D.1_cid500

Microsoft: 99,9 Prozent aller gehackten Accounts haben keine MFA
techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-tmatter/ba-p/731984#



Mitglieder der Arbeitsgruppe für Informationssicherheit der NRW Bistümer

Oliver Schröder | Bistum Aachen| Klosterplatz 7 | 52062 Aachen
informationssicherheit@bistum-aachen.de

Dirk Hennemann | Erzbistum Köln |Gereonstr. 16 | 50670 Köln
informationssicherheit@erzbistum-koeln.de

Antonio Nulchis | Bistum Münster | Magdalenenstraße 2 | 48143 Münster
informationssicherheit@bistum-muenster.de

Thomas Hoffmann| Erzbistum Paderborn | Heiersstr. 3 | 33098 Paderborn
informationssicherheit@erzbistum-paderborn.de

Bistum Essen | IT- Abteilung- Zwölfling 16 | 45127 Essen
informationssicherheit@Bistum-essen.de