Kanton Zürich
Bildungsdirektion
Mittelschul- und Berufsbildungsamt
Digital Service Center Sek II

Kontakt: Roland Brunner, Austellungsstrasse 80, 8090 Zürich
roland.brunner@edu.zh.ch

1. Juli 2022

Merkpunkte für den Aufbau und Betrieb einer sicheren IKT-Umgebung aus Sicht Datenschutz

Digitale Identitäten und Passwörter

Personalisierte Benutzeraccounts verwenden

Jede Person soll einen persönlichen Benutzeraccount erhalten, um die Nachverfolgbarkeit innerhalb der Systeme zu gewährleisten. Unpersönliche Benutzerkonten sollen auf ein Minimum reduziert und nur in Ausnahmefällen verwendet werden.

Benutzerlebenszyklus

Benutzerkonten sollen, wenn immer möglich, standardisiert und automatisiert über einen Lifecycle Prozess (Identity- und Accessmanagement) erstellt und auch wieder gelöscht werden. Dies nimmt einerseits administrative Arbeit ab und stellt zum anderen sicher, dass ausgetretene Personen auch ihren Zugriff wieder verlieren.

Rollen- und Zugriffkonzept

Zugriffe auf Daten werden rollenbasiert (und möglichst automatisiert) vergeben. Idealerweise werden diese Rollen über Gruppen (z.B. in einem Active Directory) gesteuert.
Wo Rechte manuell vergeben werden müssen (z.B. für Administratoren), sollen diese regelmässig (z.B. halbjährlich) vom Datenverantwortlichen überprüft werden.
Die Zugriffe (in Form von Rollen) sind auf das Notwendige zu beschränken (Principle of Least Privilege).

Administratoren verwenden verschiedene Benutzerkonten

Nur effektive Administrationsarbeiten werden mit Administratorenkonten /-rechten ausgeführt. Für die tägliche Arbeit ist ein Windowskonto mit normalen Benutzerrechten zu verwenden.

Administratoren-Passwörter sind seeehr stark

Für jeden Dienst muss ein separates Passwort verwendet werden. Die Länge der Passwörter beträgt mindestens 12 Zeichen und besteht aus einer Kombination aus Gross- und Kleinbuchstaben, Ziffern und Sonderzeichen. Passwörter sollen nicht im Browser gespeichert werden. Die Verwendung eines Passwortmanagers ist dringend empfohlen.

Zwei-Faktor-Authentifizierung

Administratoren nutzen IMMER Zwei-Faktor-Authentifizierung.
Wenn Dienste dies anbieten, werden diese für die Benutzenden mit Zwei-Faktor-Authentifizierung konfiguriert. Im Bereich M365 kann mit bedingten Zugriffsrichtlinien (Conditional Access) gesteuert werden wie oft und wo Zwei- bzw. Multifaktor-Authentifizierung (MFA) eingesetzt werden muss.

Systeme und Aktualität

Schwachstellen und Patchmanagement

Alle Systeme werden systematisch überwacht und auf vorhandene Schwachstellen überprüft. Spezialisierte Schwachstellen-Scanner können hier unterstützen. Patches werden zeitnah eingespielt.
Auch Hardware kennt einen Lebenszyklus. Veraltete HW muss rechtzeitig ersetzt werden.

Viren-/Malwarescanner

Ein- und ausgehender Datenverkehr (insbesondere E-Mails, surfen) sollen über isolierte Terminalserver geleitet werden. Viren-/Malwareschutz ist hier selbstverständlich.

End Point Protection

Es wird empfohlen, im E-Mail-Verkehr in Exchange Online Advanced Thread Protection mit Safe Attachments und Safe Links zu aktivieren. Im EDU-Tenant ist dies aktiviert.

Netzwerksegmentierung

Das Schulnetzwerk ist so zu segmentieren, dass Zugriffe unautorisierter Gruppen nicht ermöglicht werden.

Firewall / Proxy

Das Schulnetz und die verschiedenen Netzwerksegmente werden durch managed Firewalls / Proxy geschützt.

Unnötiges deaktivieren

Nicht benötigte Dienste, nicht verwendete Netzwerk-Ports, nicht verwendete kabellose Dienste (NFC, GPS, etc.) etc. werden deaktiviert bzw. nur bei Bedarf eingeschaltet.

(Security-)Audits
Die Infrastruktur wird regelmässig (auch durch externe Stellen) durchleuchtet (z.B. Penetrationstests).

BIOS-/Firmwareeinstellungen auf internen Geräten
Auf dem BIOS/EFI der internen Geräte sollte ein sicheres Passwort gesetzt sein.
Zudem sollten Bootoptionen für externe Medien (USB, Firewire, Thunderbolt) deaktiviert werden, da diese das Starten von portablen Systemen ermöglichen. Wenn immer möglich sollte Secureboot verwendet werden

Verschlüsselung und Datensicherung

Verschlüsselung
Der Netzwerkverkehr ist zu verschlüsseln.
Sensible Personendaten und Geschäftsgeheimnisse, vertrauliche und geheime Dokumente sind verschlüsselt abzulegen und zu versenden.

Backup
Alle geschäftsrelevanten Daten müssen regelmässig gespeichert werden. Am besten sollen Daten nach dem 3-2-1-Prinzip gesichert werden, was so viel heisst wie: von jeder Datei, welche nicht verloren gehen darf, sollen 3 Kopien existieren, 2 davon auf einem externen Medium (Festplatte, Tape, Storagesystem) mindestens 1 Kopie in einer externen Location.

Recovery
Die Datensicherungen werden periodisch auf Lesbarkeit geprüft.

Mobiles Arbeiten

BYOD
BYOD bringt viele potenziellen Gefahren mit sich. Diese können z.B. mittels Einsatz von Intune oder einer VDI (Virtual Desktop) Infrastruktur entschärft werden.
Mobile Endgeräte und Datenspeicher sind zu verschlüsseln.
Die Verwendung von Sichtschutzfolien im öffentlichen Raum (Zug, Restaurant) ist empfohlen.

Wechselmedien
Es werden nur genehmigte Wechselmedien eingesetzt. Diese müssen mit einem Passwortschutz versehen sein. Auf die fachgerechte Entsorgung ist zu achten (dies gilt auch für meinen Desktop/Laptop bzw. meine externe Festplatte und mein NAS).

VPN
Zugriffe auf das Schulnetzwerks von aussen sind über VPN zu führen. Die Authentifizierung erfolgt zuerst auf Geräte- und dann auf Benutzerebene.

Verhalten

Inventar / Risikomanagement
Ein aktuelles Hardware-, Software- und Dienste-Inventar legt die Basis, um überhaupt eine Übersicht der Risiken zu erstellen.

Notfallplan
Es ist empfohlen, einen Notfallplan für den Fall eines Datenverlustes / Angriffs oder sonstigen Sicherheitsvorfalls bereit zu halten. Dabei sind die Prozesse, Aufgaben, Kompetenzen und Zuständigkeiten und die Erreichbarkeiten festzuhalten.

Lieferanten
Lieferanten für IT-Dienstleistungen (und Systeme) sollen aktive gemanged und überwacht werden. Die Leistungen und auch die Einhaltung der Datenschutzstandards sind in Verträgen festzuhalten.

Gebäude
Es ist darauf zu achten, dass kritische Infrastrukturen nur mit besonderen Zugangsberechtigungen (Schlüssel, Badge, etc.) zugänglich sind.
Ein besonderes Augenmerk ist auf vertrauliche und geheime Informationen sowie besonders schützenswerte Personendaten zu legen.

Social Engineering
Als Administrator oder auch als Mitglied der Schulleitung bin ich mir bewusst, dass ich ein bevorzugtes Angriffsziel für Social Engineering bin. Ich bin besonders vorsichtig mit Angaben, die ich über Social Media, auf Vereinshomepages, etc. bekannt mache.
E-Mails behandle ich mit Vorsicht und klicke nicht unbedacht auf Links.

Sensibilisierung
Als IKT-Verantwortliche/r sensibilisiere ich die Benutzenden immer und immer wieder.

Tipps / Wie kann Technologie und das Digital Service Center Sek II obige Verhaltensregeln unterstützen

In der Folge haben wir lose ein paar Tipps, Links und Empfehlungen zusammengestellt, die die obenerwähnten Punkte unterstützen.

Digitale Identitäten und Passwörter		
1.	Personalisierte Benutzeraccounts	Unter Windows https://support.microsoft.com/de-de/windows/erstellen-sie-ein-lokales-benutzer-oder-administratorkonto-in-windows-20de74e0-ac7f-3502-a866-32915af2a34d Im M365 Tenant sollten ebenfalls separate Benutzeraccounts für Administratorenaufgaben erstellt werden. Diesen Accounts können dann gezielt Rechte über Rollen zugewiesen werden. https://docs.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles
2.	Benutzerlebenszyklus	Im M365-EDU-Tenant-Umfeld wird zusammen mit AFI eine IAM-Lösung eingesetzt.
3.	Rollen- und Zugriffskonzept	Erstellen eines Rollenkonzepts für die verschiedenen internen Services, in dem dokumentiert wird, welche Rollen welche Rechte innerhalb der Services / der Applikation benötigen. Im M365 Umfeld kann Privileged Identity Management (PIM) eingesetzt werden, bei dem gezielt Rollen an Administratoren verschiedener Services zugewiesen und diese nur bei Bedarf aktiviert werden. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure Unterstützung bei der Umsetzung kann das DSC Sek II auf Anfrage liefern.
4.	Administratoren verwenden verschiedene Benutzerkonten	siehe unter 1.
5.	Starke Passwörter	Die aktuellen BISR besagen: **Benutzer** **mindestens 8 Zeichen** lang sein und eine Kombination aus mindestens 3 der folgenden Kategorien enthalten: - Grossbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen **Administratoren** **mindestens 12 Zeichen** lang sein und eine Kombination aus mindestens 3 der folgenden Kategorien enthalten: - Grossbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen Am besten das Passwort von einem Generator erstellen lassen und dieses in einem Passwortmanager verschlüsselt abspeichern. **Empfohlene Passwortmanager**: https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_passwortmanager.pdf **KeePass2**, LastPass, SecureSafe Prüfung, ob ein Passwort von einem Passwort-Klau betroffen war: https://www.ibarry.ch/de/sicherheits-checks/

6.	2-Faktor- bzw. Multifaktor Authentifizierung	2-Faktor-Authentifizierung ist bei allen Diensten zu aktivieren, die dies zulassen und wo Personendaten bearbeitet werden. Die Nutzung einer Authenticator-App (bevorzugt Microsoft) wird einer SMS-Authentifizierung vorgezogen. Ebenfalls für den Zugriff auf die Infrastruktur von ausserhalb des Schulnetzes soll 2FA verwendet werden. Aktivieren Sie MFA auf Ihrem M365 Tenant, Erzwingen Sie dies für alle Adminbenutzer und wenn möglich auch für alle Benutzenden. Über bedingte Zugriffrichtlinien, kann MFA gezielt und auch situativ forciert und die Intervalle zwischen einer erneuten MFA Authentifizierung gesteuert werden. Set up multifactor authentication for users - Microsoft 365 admin | Microsoft Docs
Systeme und Aktualität		
7.	Schwachstellen und Patchmanagement	Aktuelle Informationen: https://www.trendmicro.com/de_de/security-intelligence/breaking-news.html
8.	Viren-/Malwarescanner	MBA verfügt einen Rahmenvertrag mit SOPHOS. SOPHOS kann über das Service Desk DSC II bezogen worden. SOPHOS kann auch (gratis) für bis zu 10 private Geräte eingesetzt werden.
9.	End Point Protection	Im M365-EDU-Tenant ist dies bereits aktiviert. Ansonsten besteht die Möglichkeit, SOPHOS Home Lizenzen bei DSC zu bestellen (kostenpflichtig).
10.	Netzwerksegmentierung	Im LEUNET ist die Netzwerksegmentierung umgesetzt. Info über Netzwerksegmentierung: https://www.ip-insider.de/wie-netzwerksegmentierung-fuer-mehr-sicherheit-sorgt-a-794444/
11.	Firewall / Proxy	Die Möglichkeiten einer Firewall sind Herstellerabhängig sehr verschieden. Wir empfehlen, sich mit den Möglichkeiten auseinander zu setzen und möglichst vielfältig einzusetzen. Ein paar Tipps: Geoblocking aktivieren, DMZ, Black-/White-Lists, Content Blocking. Auf Endgeräten: Win Defender Firewall nutzen DSC kann hier unterstützen. Kontakt über Service Desk.
12.	Dienste / Netzwerkports deaktivieren	Grundsätzlich soll alles «geschlossen/nicht erlaubt» sein, was nicht verwendet wird (Protokolle, Ports, Dienste, etc.). Informationen bei den jeweiligen Herstellern bzw. Dienstleistern.
13.	(Seucrity-) Audits	Audits durch externe Stellen bieten eine gute Möglichkeit. Aktuell ist DSC daran, mit Swisscom ein Standardauditing aufzubauen (primär Netzwerksicherheit, Serverhardening, Endgeräte). Für Beratung wenden Sie sich bitte an das DSC. Es gibt auch die Möglichkeit von Self-Assessments wie IKT-Resilienzcheck. Siehe https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html
14.	BIOS- / Firmwareeinstellungen auf internen Geräten	Siehe im Text oben.
Verschlüsselung und Datensicherung		
15.	Verschlüsselung	Wenn immer möglich sollte eine Festplattenverschlüsselung z.B. Bitlocker aktiviert werden. Der Netzwerkverkehr bei M365 ist standardmässig verschlüsselt. Webservices über Port 443 (https statt http) anbieten. Mail: - Innerhalb M365 kann die Microsoft-Verschlüsselung verwendet werden.

		- Verwendung von Inca-Mail zur Mailverschlüsselung Vertrauliche Dokumente nur verschlüsselt versenden oder in Cloud-Diensten wie OneDrive, Sharepoint abspeichern.
16.	Backup	M365 Tenant wird von Seite DSC gesichert. Wichtige Geschäftsdaten sollen nicht lokal gespeichert werden, sondern auf Servern oder Cloud.
17.	Recovery	Backups testen, auf Wiederherstellbarkeit und Lesbarkeit.
Mobiles Arbeiten		
18.	BYOD	Ein paar Tipps: Geräte-Login und Bildschirmsperre aktivieren, Sichtschutzfolien einsetzen, Lokale Daten sichern, auch hier unterschiedliche Benutzerkonten verwenden
19.	Wechselmedien	Möglichst vermeiden mit USB-Sticks zu arbeiten.
20.	VPN	Heute werden eingesetzt: In Mittelschulen: SOPHOS VPN-Tunnel In Berufsfachschulen: Citrix oder sRAS Bei Bedarf unterstützt das DSC.
Verhalten		
21.	Inventar-/Risiko-management	Tipp: Erarbeiten eines Datenbearbeitungsverzeichnisses. Einsatz einer Netzwerk-Überwachung-Software wie PRTG.
22.	Notfallplan	Wichtigste Adresse, Telefonnummern, etc. sollen auch physisch (Papierform) vorhanden sein. Der Notfallplan ist regelmässig «zu üben»; Kontrolle der Aktualität der Telefonnummer, etc., Kontrolle der Prozesse und Zuständigkeiten. Sicherheitsvorfall: Es hat sich bewährt, rasch alle möglichen Stellen (z.B. DSC, AFI) einzubeziehen. Zudem besteht eine Meldepflicht von Cybersecurity-Vorfällen (Kantonale Datenschützerin, Bund / NCSC).
23.	Lieferanten	https://datenschutz.ch/lexika/volksschule/auslagerung (gilt auch für die Mittel- und Berufsschulen) https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf
24.	Gebäude	Switches, Stockwerkverteiler, etc. dürfen nicht offen in Schulzimmern oder dergleichen stehen, sondern abschliessbar in einem Rack oder einem separaten Raum.
25.	Social Engineering	Ein sehr spannender Film zu Social Engineering: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html
26.	Sensibilisierung	Von Seiten Kanton und MBA wird in den nächsten Monaten eine Kampagne vorbereitet und durchgeführt. Diese soll auch durch die Schulen genutzt werden können. Für den Unterricht: Ein Phishing-Test: https://www.ebas.ch/phishing-test/ Video der Post zu Phishing (französisch mit deutschen Untertiteln): https://www.youtube.com/watch?v=yeQnWBAdiEE oder https://www.youtube.com/watch?v=XgF42Jb8jxo