2012

IT-Sicherheitsrichtlinie

IT-Sicherheitsrichtlinie des SBSZ Jena-Göschwitz

Die IT-Sicherheitsrichtlinie wurde am 13. Juni 2012 von der Schulkonferenz des Staatlichen Berufsbildenden Schulzentrums Jena-Göschwitz verabschiedet und ist seit dem Zeitpunkt in Kraft. Die Richtlinien sind dementsprechend für alle verbindlich. Ein Ablaufdatum wurde noch nicht festgelegt, ist aber empfehlenswert. Dadurch lässt sich verhindern, dass einige Richtlinien im Laufe der Zeit formell außer Kraft treten könnten, da diese nicht mehr aktuell sind.

Inhaltsverzeichnis

I. Überblick 2

II. Geltungsbereich 2

III. Umsetzung 2

IV. Richtlinien 3

1. Fokus 3

1.A Benutzer 3

1.B Administratoren 3

1.C Datensicherung 3

2. Mindeststandards für den Betrieb eines Computers 4

3. Mindeststandards für den Betrieb eines Netzes 5

4. Regelwidrige Benutzung 6

4.A Verwendung elektronischer Kommunikation für Angriffe gegen Einzelpersonen oder Gruppen von Personen 6

4.B Verwendung elektronischer Kommunikation zur Behinderung der Arbeit Dritter 6

4.C Vergehen gegen Lizenzvereinbarungen oder andere vertragliche Bestimmungen 6

4.D Verwendung elektronischer Kommunikation für Attacken gegen Computer, das Netz oder *Services*, die darauf erbracht werden 7

5. Konsequenzen bei Nichteinhaltung der Sicherheitsrichtlinie 8

5.A Maßnahmen durch den Systemadministrator 8

5.B Maßnahmen durch die Schulbibliothek 9

I. Überblick

Das Staatliche Berufsbildende Schulzentrum (SBSZ) Jena-Göschwitz ist eine Schule mit ca. 2000 Schülern, ca. 120 Lehrkräften und ca. 15 Mitarbeitern, bei der das Wissen in den unterschiedlichen Schulformen zielorientiert und planmäßig vermittelt wird. Es werden neue Lernmethoden verwendet und da wir in einem Zeitalter des Internets leben, sind Computer aus allen Bereichen der Wissensvermittlung gar nicht mehr wegzudenken. So ist in einigen Schulformen der Gebrauch von Computern und Netzen zur Routine geworden. Computer erleichtern das Arbeiten an bestimmten Projekten/Aufgaben, da einige Ausarbeitungen digital angefertigt werden müssen. Damit die ordnungsgemäße Benutzung gewährleistet und fahrlässige oder gar gesetzwidrige Verwendung ausgeschlossen wird, müssen bestimmte Richtlinien eingehalten werden. Es wird ein verantwortungsbewusster Umgang bei dem Gebrauch von Computern und Netzen erwartet, welcher bei Verstößen gegen die Sicherheitsrichtlinie oder gegen gesetzliche Bestimmungen geahndet wird.

II. Geltungsbereich

Die IT-Sicherheitsrichtlinie ist entscheidend zur Steigerung von Datenschutz und Datensicherheit und dementsprechend für jeden Angehörigen (Schüler, Auszubildende, Lehrkräfte, Mitarbeiter, Leiter) sowie Personen, denen durch Berechtigung die Benutzung von IT-Systemen möglich ist, verbindlich. Darüber hinaus bildet sie die Grundlage für Reaktionen auf alle sicherheitsrelevanten Vorfälle von außerhalb.

III. Umsetzung

Es müssen Fristpläne erstellt werden, welche besonders bei neuen Regelungen strikt einzuhalten sind. Neue Vorschriften sollen genau festgelegt werden, bei denen stets ein Verantwortlicher zu benennen ist (Nutzer, Administratoren, Führungskräfte,…). Sicherheitsmaßnahmen sind mit den Verantwortlichen zu besprechen und es sollte auf indirekte Gefahren verwiesen werden. Es ist auch empfehlenswert, eine ausführliche Maßnahmenbeschreibung als Umsetzungshilfe anzulegen.

IV. Richtlinien

Die nachfolgenden Maßnahmen sollen die Sicherheit fördern.

1. Fokus

1.A Benutzer

- Benutzer sollten sich über Änderungen an der Sicherheitsrichtlinie auf dem Laufenden halten.
- Erforderliche Aktionen auf Grund einer Änderung der Sicherheitsrichtlinie sind umgehend durchzuführen.
- Verstöße oder vermutete Verstöße gegen die Sicherheitsrichtlinie sind umgehend dem Systemadministrator mitzuteilen.
- Eine regelmäßige Teilnahme an Schulungen zum Thema IT-Sicherheit wird empfohlen.

1.B Administratoren

- Alle Maßnahmen der Benutzer und zusätzlich
  - Informieren der Benutzer über sicherheitsrelevante Vorfälle, Bedrohungen usw.
  - Schulung der Benutzer, insbesondere über relevante Themen zur Erhaltung und Erhöhung der IT-Sicherheit (auch für neue Benutzer).
  - Informieren über Schwachstellen und Bedrohungen in der eingesetzten Software.

1.C Datensicherung

Verantwortlich für das Sichern der eigenen Daten ist jeder Benutzer selbst.

Daten in gemeinsam genutzten Ordnern (z. B. Austausch) und auf dem Exchange-Server (E-Mail, Kalender) werden zentral durch die Administratoren gesichert.

2. Mindeststandards für den Betrieb eines Computers

Um den ordnungsgemäßen Betrieb eines Computers oder einer aktiven Netzkomponente zu gewährleisten, müssen mindestens die folgenden Anforderungen erfüllt sein.

1. Das System muss fachgerecht installiert werden.

2. Die notwendigen *Security Patches* oder *Upgrades* müssen zeitnah installiert werden.

3. Falls ein System nicht über geeignete Schutz-Mechanismen verfügt, muss es netzwerkseitig geschützt werden, z. B. durch eine *Firewall*.

4. Nicht mehr verwendete Benutzerzugänge müssen entfernt werden.

5. Passwörter müssen regelmäßig geändert werden und es müssen sichere Passwörter oder stärkere Authentifizierungsmethoden (z. B. *Public Key*) benutzt werden.

6. Passwörter dürfen nicht im Klartext über die Grenzen des Schulnetzes versendet werden und sollten auch innerhalb des Schulnetzes nach Möglichkeit nicht im Klartext übertragen werden.

7. Passwörter sollten niemals auf der Festplatte gespeichert werden, um deren Eingabe in einem Programm zu umgehen.

8. Wird ein Verfahren eingeführt oder wesentlich geändert, in dem personenbezogene Daten verarbeitet werden, ist ein Verfahrensverzeichnis nach § 10 ThürDSG zu erstellen. Das Ergebnis ist der Schulleitung des SBSZ Jena-Göschwitz zuzusenden.

Falls einem Benutzer eines Computers Sicherheitsmängel auffallen, ist er **verpflichtet**, die Mängel dem Systemadministrator des SBSZ Jena-Göschwitz zu melden. Der Systemadministrator ist verpflichtet, ihm bekannte bzw. bekannt gemachte Informationen über Sicherheitsmängel eines Computers an den zuständigen Administrator weiterzuleiten. Der Administrator ist verpflichtet, geeignete Gegenmaßnahmen zu ergreifen.

3. Mindeststandards für den Betrieb eines Netzes

Ein Netzbetrieb im Sinne dieser Richtlinie liegt dann vor, wenn dedizierte Netzwerk-Hardware (z. B. *Router*) betrieben wird oder auf logischer Ebene Netzwerkdienste angeboten werden, wie z. B. *DNS*- oder *DHCP-Server*.

1. Zu jedem Bereich (Subnetz, IP-Bereich, DNS-Domäne) ist mindestens eine verantwortliche Person zu benennen (besser mehrere Personen, so dass im Falle von Fehlern oder Sicherheitsvorfällen immer eine verantwortliche Person erreicht werden kann), die auch technisch in der Lage ist, Notmaßnahmen durchzuführen.

2. Der Zugang zum Netz darf nicht unkontrolliert erfolgen. Der Netzzugang muss physikalisch und administrativ durch Zugriffslisten, VPN-Zugang o. ä. geregelt sein.

3. Es muss nachvollziehbar sein, wer bzw. welches Gerät eine IP-Adresse zu einer bestimmten Zeit hatte.

4. Die Standorte aller im Netz befindlichen Komponenten, auch die der angeschlossenen Rechner, müssen den verantwortlichen Personen bekannt sein.

5. Die Namen und / oder Adressen der Netzwerkkomponenten (einschließlich der Rechner) sollten außen am Gerät sichtbar sein.

4. Regelwidrige Benutzung

Die in der Sicherheitsrichtlinie festgelegten Regelverstöße sind thematisch in vier Bereiche gegliedert. Strafrechtlich sanktioniertes Verhalten ist immer regelwidrig.

4.A Verwendung elektronischer Kommunikation für Angriffe gegen Einzelpersonen oder Gruppen von Personen

A1) Verbreitung oder In-Umlauf-Bringen von Informationen, die Personen beleidigen oder herabwürdigen (z. B. aufgrund ihrer Hautfarbe, Nationalität, Religion, ihres Geschlechtes, ihrer politischen Gesinnung oder sexuellen Ausrichtung).

A2) Unbefugte Verarbeitung personenbezogener Daten und Verbreitung von persönlichen oder anderen schützenswerten Informationen über eine Einzelperson oder eine Gruppe von Personen.

A3) Mehrfach unerwünschtes Zusenden von Nachrichten.

4.B Verwendung elektronischer Kommunikation zur Behinderung der Arbeit Dritter

B1) Behinderung der Arbeit anderer (z. B. durch *Mail*-Bomben und ähnliche Techniken).

B2) Aneignung von Ressourcen über das zugestandene Maß (z. B. extremer Datenverkehr).

B3) Versenden von elektronischen Massensendungen (z. B. *SPAM E-Mails*). Ausnahme: Verbreitung von dienstlichen Mitteilungen in Analogie zur Hauspost.

B4) Weitersenden oder In-Umlauf-Bringen von elektronischen Kettenbriefen.

B5) Unberechtigte Manipulation von elektronischen Daten anderer.

B6) Zugriff auf Daten Dritter ohne deren Erlaubnis.

4.C Vergehen gegen Lizenzvereinbarungen oder andere vertragliche Bestimmungen

C1) Die Nutzung, das Kopieren und Verbreiten von urheberrechtlich geschütztem Material im Widerspruch zum Urheberrechtsgesetz, zu Lizenzvereinbarungen oder anderen Vertragsbestimmungen auf Computern des SBSZ Jena-Göschwitz bzw. der Transport dieser Dokumente über Netze des SBSZ Jena-Göschwitz.

C2) Verletzung des Urheberrechts durch Verfälschung elektronischer Dokumente.

C3) Weitergabe von Zugangsberechtigungen an Dritte (z. B. *Accounts*, Passwörter)

4.D Verwendung elektronischer Kommunikation für Attacken gegen Computer, das Netz oder *Services*, die darauf erbracht werden

Für die nachfolgenden Verstöße besteht eine **Meldepflicht** an den Systemadministrator des SBSZ Jena-Göschwitz!

D1) Systematisches Ausforschen von *Servern* und *Services* (z. B. *Port Scans*). Ausnahme: Sicherheitstests nach Absprache mit dem Systemadministrator.

D2) Unerlaubte Aneignung von Zugangsberechtigungen oder der Versuch einer solchen Aneignung (z. B. *Cracken*). Ausnahme: Sicherheitstests nach Absprache mit dem Systemadministrator.

D3) Beschädigung oder Störung von elektronischen Diensten (z. B. *Denial-of-Service-Attacks*).

D4) Vorsätzliche Verbreitung oder In-Umlauf-Bringen von schädlichen Programmen (z. B. Viren, Würmer, Trojanische Pferde).

D5) Ausspähen von Passwörtern oder auch der Versuch des Ausspähens (z. B. *Password Sniffer*).

D6) Unberechtigte Manipulation oder Fälschung von Identitätsinformationen (z. B. *E-Mail-Header*, elektronische Verzeichnisse, *IP-Spoofing*, etc.).

D7) Ausnutzen erkannter Sicherheitsmängel bzw. administrativer Mängel.

5. Konsequenzen bei Nichteinhaltung der Sicherheitsrichtlinie

Die meisten Verstöße resultieren erfahrungsgemäß aus Unkenntnis der Sicherheitsrichtlinie oder technischer Unzulänglichkeit. In solchen Fällen wird es ausreichen, wenn der Verursacher über den Verstoß gegen die Sicherheitsrichtlinie des SBSZ Jena-Göschwitz aufgeklärt und die Unterlassung weiterer Verstöße gefordert wird. Bei Verstößen gegen Lizenzvereinbarungen muss gegebenenfalls die Löschung der entsprechenden Daten auf den betroffenen Rechnern verlangt werden. Wenn anzunehmen ist, dass erkannte Verstöße auch andere Abteilungen, Fachbereiche, Einrichtungen oder Organisationen (auch außerhalb des SBSZ Jena-Göschwitz) betreffen könnten, sind die betreffenden Verantwortlichen und eventuell auch die Schulleitung des SBSZ Jena-Göschwitz zu informieren (z. B. Sperren eines Benutzers, der auch über Zugangsberechtigungen auf anderen Computern verfügt).

Falls die direkte Aufforderung ohne Erfolg bleibt oder die Identität des Verursachers nicht festgestellt werden kann, ist die Schulleitung des SBSZ Jena-Göschwitz in die Lösung des Problems mit einzubeziehen.

Neben der Beschreibung des Problems sollte immer explizit angeführt werden, gegen welchen Punkt der Sicherheitsrichtlinie verstoßen wurde. Bei Uneinigkeit über die Richtigkeit der Beschwerde entscheidet der Systemadministrator des SBSZ Jena-Göschwitz und in zweiter Instanz die Schulleitung.

5.A Maßnahmen durch den Systemadministrator

1. Der Systemadministrator wird den für das Netz oder den Rechner Verantwortlichen auffordern, Regelverstöße zu unterbinden, gegebenenfalls die Zugangsberechtigung des Verursachers zu sperren sowie bei Verstößen gegen Lizenzvereinbarungen die betreffenden Informationen von den Rechnern zu löschen.
2. Ist der jeweilige Verantwortliche nicht erreichbar oder nicht imstande bzw. nicht bereit, solche Verstöße zu verhindern, so ist der Systemadministrator verpflichtet, die Schulleitung von den Missständen zu informieren. Die Schulleitung wird den Verantwortlichen zur Behebung des Verstoßes auffordern.
3. Bleibt auch die Maßnahme in Punkt 2 ohne Erfolg, so ist der Systemadministrator berechtigt, den betreffenden Rechner aus dem Netz zu entfernen bzw. die betreffenden *Services* oder ggf. ein ganzes Subnetz zu sperren.
4. Wenn die Umstände es verlangen (Gefahr in Verzug), können Sperren vom dem Systemadministrator auch ohne Rücksprache mit dem jeweiligen Verantwortlichen vollzogen werden. Der Systemadministrator ist in solchen Fällen verpflichtet, die Betroffenen (soweit dies möglich ist) und die Schulleitung unmittelbar danach über die getroffenen Maßnahmen zu informieren.
5. Strafrechtlich relevante Vorfälle sind, z. B. wegen eventueller Schadensersatz-forderungen für Schäden, grundsätzlich an die Schulleitung des SBSZ Jena-Göschwitz weiterzuleiten.
6. Zusätzlich kann vom Verursacher die schriftliche Kenntnisnahme der IT-Sicherheitsrichtlinie verlangt werden.

5.B Maßnahmen durch die Schulbibliothek

Die Maßnahmen der Schulbibliothek sind in der "Benutzungsordnung der Schulbibliothek des SBSZ Jena-Göschwitz“ geregelt.