Universität Bielefeld

IT-Sicherheitsrichtlinie zur Handhabung von IT-Sicherheitsvorfällen

Referenznummer	IT-SEC RL010
Titel	IT-Sicherheitsrichtlinie zur Handhabung von IT-Sicherheitsvorfällen
Zielgruppe	IT-Personal, Mitarbeiterinnen und Mitarbeiter
Version	1.0
Status des Dokuments	Verabschiedet
Gültig seit	13.05.2015
Letzte Änderung	07.05.2015
Nächste Revision	14.05.2016
Autor / Besitzer des Dokuments	IT-Sicherheitsbeauftragter (Michael Sundermeyer)
Verabschiedet durch	Sicherheitsmanagement-Team (SMT)
Implementiert durch	IT-Sicherheitsbeauftragter
Monitoring der Einhaltung	Bereichs-IT-Sicherheitsbeauftragte (BITS)
Kommentare	

1. Einführung

Die Universität Bielefeld ist in hohem Maße auf die Verfügbarkeit, Vertraulichkeit und Integrität ihrer Informationstechnologie (IT) angewiesen. Die vorliegende IT-Sicherheitsrichtlinie definiert organisatorische Maßnahmen bei der Handhabung von IT-Sicherheitsvorfällen, die notwendig sind, um die Daten der Universität zu jedem Zeitpunkt angemessen zu schützen.

2. Geltungsbereich

Diese Richtlinie gilt für das IT-Personal sowie alle Beschäftigten, die die IT-Dienste oder Daten der Universität Bielefeld nutzen.

3. Zuständigkeiten

Die Leitungen der Fakultäten und Einrichtungen stellen sicher, dass die Beschäftigten in ihrem Bereich über diese Richtlinie in Kenntnis gesetzt werden und die Möglichkeit haben, IT-Sicherheitsvorfälle zu melden. Die jeweiligen Bereichs-IT-Sicherheitsbeauftragten (BITS) überwachen im Auftrag der Leitungen die Umsetzung und Einhaltung dieser Richtlinie.

4. Regelungen

4.1 Definition

Ein IT-Sicherheitsvorfall ist gekennzeichnet durch den Verlust von Verfügbarkeit, Integrität oder Vertraulichkeit von IT-Diensten oder Daten der Universität Bielefeld. Dazu zählen beispielsweise Phishing- oder Denial-of-Service-Angriffe, Infektion mit Schadsoftware, unautorisierte Zugriffe etc. Auch der Versuch dies durchzuführen, kann einen IT-Sicherheitsvorfall darstellen. Ausgenommen ist technisches Versagen ohne Fremdeinwirkung. Weitere Beispiele für IT-Sicherheitsvorfälle sind im Abschnitt 4.4 beschrieben.

4.2 Meldung von IT-Sicherheitsvorfällen durch die Beschäftigen

- Beschäftigte der Universität Bielefeld, die von einem IT-Sicherheitsvorfall Kenntnis erhalten, informieren die zuständige EDV-Betreuung sofort persönlich, per Telefon oder E-Mail. Ist diese nicht ansprechbar, ist der oder die DV-Beauftragte des Bereichs zu informieren.

Ansprechfall	Ansprechpersonen/Bereich	Kontakt
Jeder IT-Sicherheitsvorfall	EDV-Betreuung der Fakultät oder Einrichtung	In der Personensuche (PEVZ) der Universität unter dem Menüpunkt „Ansprechpersonen“
Wenn die EDV-Betreuung nicht ansprechbar ist (Vertretung)	DV-Beauftragte der Fakultät oder Einrichtung	In der Personensuche (PEVZ) der Universität unter dem Menüpunkt „Ansprechpersonen“

4.3 Behandlung von IT-Sicherheitsvorfällen durch die EDV-Betreuung

Der folgende Ablauf dient als generischer Rahmen zur Handhabung von IT-Sicherheitsvorfällen:

- Klassifizierung des IT-Sicherheitsvorfalls auf Basis der Kategorien (vgl. Abschnitt 4.4 Teil A)
- Dringlichkeit der Bearbeitung des IT-Sicherheitsvorfalls basierend auf dessen Schwere priorisieren (vgl. Abschnitt 4.4 Teil B)
- Eindämmung des IT-Sicherheitsvorfalls, indem notwendige technische und organisatorische Schritte unternommen werden, um eine weitere Eskalation der Ereignisse zu verhindern.

- Melden des IT-Sicherheitsvorfalls an die notwendigen Personen (vgl. Abschnitt 4.5)
- Betroffenes IT-System wieder in einen funktionsfähigen und sicheren[1] Zustand bringen
- Prüfen, ob die Ursache des Vorfalls vollständig beseitigt wurde und ob das IT-System wieder einschränkungsfrei funktioniert
- Sofern notwendig weitere technische und organisatorische Maßnahmen zur zukünftigen Sicherstellung von Verfügbarkeit, Integrität und Vertraulichkeit umsetzen (Anpassung von Updateprozessen, zusätzliches Monitoring etc.)
- Abschließende Dokumentation des IT-Sicherheitsvorfalls erstellen (vgl. Abschnitt 4.7)

4.4 Klassifizierungen von IT-Sicherheitsvorfällen

IT-Sicherheitsvorfälle sind durch die EDV-Betreuungen der Fakultäten und Einrichtungen zu klassifizieren. Der Umgang mit den Vorfällen erfolgt auf Basis dieser Einstufung:

A. Kategorien

Die folgenden Kategorien werden genutzt, um IT-Sicherheitszwischenfälle an der Universität Bielefeld zu beschreiben. Die Beispiele in den einzelnen Kategorien sind nicht erschöpfend:

a. Denial of Service (DoS)
   - Einfach oder verteilt (DoS oder DDos)
   - Eingehend oder ausgehend
   - Sonstiges

b. Schadsoftware/-hardware
   - Wurm, Virus oder Trojaner
   - Bot-Netz
   - Keylogger
   - Rootkit
   - Sonstiges

c. Scan/Monitoring
   - Unautorisiertes Port Scanning
   - Unautorisiertes Vulnerability Scanning
   - Unautorisiertes Monitoring / Überwachung von Netzwerkaktivitäten
   - Sonstiges

d. Spam
   - Massenversand von IP-Adresse der UniBi
   - Massenversand über smtp-Relays der UniBi
   - Zustellung von Extern
   - Sonstiges

e. Phishing
   - Allgemeines Phishing
   - Spear Phishing (gezielter Versand von Phishing-E-Mails an ausgewählte Personen)
   - Sonstiges

f. Social Engineering (zwischenmenschliche bzw. soziale Manipulation von Personen, um an vertrauliche Daten zu gelangen)

g. Bösartiger Server oder Service im Netz der Universität
   - Botnetz-Kontroll-Server
   - Webserver für Phishing-Aktivitäten
   - Server mit Material, welches gegen das Urheberrecht verstößt

[1] Vgl. Regelungen zum IT-Basisschutz für das IT-Personal, insbesondere die Maßnahme M 2.28.

- Bösartiger WLAN Access Point
- Sonstiges

h. Unautorisierter Zugriff
- Missbrauch oder Erschleichung von Zugriffsberechtigungen
- Unautorisierter Zugriff auf vertrauliche Daten
- Systematischer unautorisierter Login-Versuch
- Brute Force-Versuch
- Passwort Diebstahl
- Unautorisierte Weitergabe von Zugangsdaten
- Schwaches oder kein Passwort auf Account gesetzt
- Sonstiges

i. Unautorisierter Zutritt (zum Beispiel zu Serverräumen)
- Einbruch
- Missbrauch oder Erschleichung von Schlüsseln oder Schließkarten
- Unautorisierte Weitergabe von Schlüsseln oder Schließkarten
- Verstoß gegen Zutrittsregelungen
- Sonstiges

j. Sicherheitslücke
- Nicht geschlossene Sicherheitslücke in Betriebssystem
- Nicht geschlossene Sicherheitslücke in Anwendung
- Nicht geschlossene Sicherheitslücke in Internetseite/Service
- Sonstiges

k. Sonstiges (wenn keine Zuordnung möglich ist)

B. Schwere des IT-Sicherheitsvorfalls bestimmen

Die Schwere eines Vorfalls ist ein subjektives Maß, um die Auswirkungen auf (und die Bedrohung für) die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Dienste und Daten der Universität zu ermitteln. Die Einstufung legt fest, mit welcher Priorität und in welchem Umfang auf den Vorfall reagiert werden muss.

Beispiel: Über eine Sicherheitslücke im Betriebssystem wird ein Server angegriffen und kompromittiert. Auf dem Server befindet sich der Internetauftritt der Fakultät, welcher über ein Content Management System gepflegt wird. Durch die Manipulationen des Systems ist dessen Integrität und die Integrität der verarbeiteten Daten nicht länger gewährleistet. Um die Integrität wiederherzustellen, muss der Server neu installiert werden. In diesem Zeitraum steht der Internetauftritt der Fakultät nicht zur Verfügung. Da der Internetauftritt Daten enthält, die für die Arbeit der Fakultät wichtig sind, wird dadurch die Aufgabenerfüllung des Teilbereichs eingeschränkt.
In diesem Fall würde der IT-Sicherheitsvorfall in der Kategorie „Beeinträchtigung der Aufgabenerfüllung“ in die mittlere Stufe eingeordnet werden. Ergeben sich in den anderen Kategorien keine höheren Einstufungen, wäre die Schwere des Vorfalls insgesamt als mittel einzustufen.

Die folgende Tabelle dient als Vorlage für eine Einstufung. Ziel ist es, anhand der Beispiele die Schwere der Auswirkungen zu ermitteln. Die Beeinträchtigungen durch den IT-Sicherheitsvorfall sind anhand der fünf aufgeführten Felder zu betrachten. Die höchste Einstufung ist ausschlaggebend für die Gesamteinstufung des IT-Sicherheitsvorfalls:

Beeinträchtigungen	Schwere des IT-Sicherheitsvorfalls		
	Niedrig	**Mittel**	**Hoch**
1. Beeinträchtigung der Aufgabenerfüllung	…führt maximal zum Ausfall **einzelner** Arbeitsabläufe (tolerierbare Ausfallzeit mehr als einen Arbeitstag).	…schränkt die Aufgabenerfüllung in einem **Teilbereich** ein (tolerierbare Ausfallzeit zwischen einer und 24 Stunden).	…gefährdet den **Gesamtauftrag** der Universität (tolerierbare Ausfallzeit weniger als eine Stunde).
2. Negative Innen- und Außenwirkung	…könnte höchstens zu **geringem** Ansehens- und Vertrauensverlusts eines Teilbereichs der UniBi bei einer **eingeschränkten** Öffentlichkeit führen	... könnte zu einem Ansehens- und Vertrauensverlusts der UniBi bei einer **eingeschränkten** Öffentlichkeit oder einem **hohen** Ansehensverlust eines Teilbereichs der UniBi führen	... könnte zu einem **landesweiten** Ansehens und Vertrauensverlust der UniBi in der **breiten** Öffentlichkeit führen
3. Finanzielle Auswirkungen	Geschätzte Summe der finanziellen Auswirkungen weniger als 150.000 Euro (Summe ist ein Orientierungsrahmen)	Geschätzte Summe der finanziellen Auswirkungen weniger als 3 Millionen Euro (Summe ist ein Orientierungsrahmen)	Geschätzte Summe der finanziellen Auswirkungen mehr als 3 Millionen Euro (Summe ist ein Orientierungsrahmen)
4. Beeinträchtigung des Informationellen Selbstbestimmungsrechts (Datenschutz)	…kann durch Betroffene als **tolerable** Beeinträchtigung des informationellen Selbstbestimmungsrechts eingeschätzt werden. Ein Missbrauch personenbezogener Daten hätte nur **geringfügige** Auswirkungen auf die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse Betroffener.	...könnte zu einer **erheblichen** Beeinträchtigung des informationellen Selbstbestimmungsrechts Einzelner führen. Ein Missbrauch personenbezogener Daten hätte **erhebliche** Auswirkungen auf die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse Betroffener.	...könnte zu einer **gravierenden** Beeinträchtigung des informationellen Selbstbestimmungsrechts Einzelner führen. Ein Missbrauch personenbezogener Daten könnte für Betroffene den gesellschaftlichen und/oder wirtschaftlichen Ruin bedeuten (Gefahr für Leib und Leben oder persönliche Freiheit).
5. Verstoß gegen Gesetze, Vorschriften und/oder Verträge	...könnte mit **geringen** Konsequenzen gegen Gesetze oder Vorschriften verstoßen. ...könnte **geringfügige** Vertragsverletzungen mit maximal geringen Konventionalstrafen zur Folge haben.	...könnte mit **erheblichen** Konsequenzen gegen Gesetze oder Vorschriften verstoßen. ...könnte Vertragsverletzungen mit **hohen** Konventionalstrafen und/oder erheblichen Haftungsschäden zur Folge haben.	...könnte **fundamental** gegen Gesetze oder Vorschriften verstoßen. ...könnte Vertragsverletzungen zur Folge haben, deren Haftungsschäden für die UniBi **ruinös** sind.
Beeinträchtigungen	**Niedrig**	**Mittel**	**Hoch**

Die Einstufung eines Vorfalls kann bei Bedarf, beispielsweise durch die Gewinnung neuer Erkenntnisse, jederzeit durch die EDV-Betreuung angepasst werden. Dies ist entsprechend zu dokumentieren (vgl. Abschnitt 4.7).

4.5 Melden von IT-Sicherheitsvorfällen durch die EDV-Betreuung

- Der oder die zuständige EDV-Betreuer/Betreuerin bzw. dessen Stellvertretung informiert über jeden Vorfall, welcher als „mittel“ und „hoch“ eingestuft wird (vgl. Abschnitt 4.3, Teil B), umgehend den oder die IT-Sicherheitsbeauftragte/n. Ist dieser nicht ansprechbar, ist der Chief Information Officer (CIO) zu informieren.
- Der oder die IT-Sicherheitsbeauftragte/n informiert (sofern noch nicht geschehen) den Chief Information Officer (CIO) und ggf. weitere Personen über den Vorfall (siehe Abschnitt 4.6 Security Incident Management Team).
- Anfragen der Presse zu IT-Sicherheitsvorfällen sind an die Pressestelle der Universität zu verweisen.

Ansprechfall	Ansprechpersonen/Bereich	Kontakt
IT-Sicherheitsvorfälle mit einer mittleren oder hohen Einstufung sowie Fragen zu dieser Richtlinie	IT-Sicherheitsbeauftragte/r	it-sicherheit@uni-bielefeld.de Durchwahl: -12100
Wenn die bzw. der IT-Sicherheitsbeauftragte nicht erreichbar ist (Vertretung)	Chief Information Officer (CIO)	frank.klapper@uni-bielefeld.de Durchwahl: -4954

4.6 Security Incident Management Team

Das Security Incident Management Team (SIMT) ist für eine Begleitung und Beratung von als „hoch“ eingestuften IT-Sicherheitsvorfällen verantwortlich. Das SIMT wird durch die oder den IT-Sicherheitsbeauftragte/n ad hoc und situationsangemessen zusammengerufen.
Es besteht im Allgemeinen aus:

- Einer oder einem Vertreter/in der EDV-Betreuung des betroffenen Bereichs
- Der oder dem Chief Information Officer (CIO)
- Der oder dem Datenschutzbeauftragten (sofern personenbezogene Daten betroffen sind)
- Der oder dem IT-Sicherheitsbeauftragten
- Einer oder einem Vertreter/in des Justiziariats
- Einer oder einem Vertreter/in des Referats für Kommunikation
- Weitere Beschäftigte sofern notwendig (beispielsweise sachverständige Vertreter zentraler IT-Dienstleister)

4.7 Dokumentation von IT-Sicherheitsvorfällen

Zur Gewährleistung einer Nachvollziehbarkeit von IT-Sicherheitsvorfällen, sind als mittel oder hoch eingestufte Vorfälle schriftlich in angemessenem Umfang durch die EDV-Betreuung zu dokumentieren.
Zu einem Vorfall sollten mindestens folgende Informationen festgehalten werden:

- Kurzbezeichnung
- Detaillierte Beschreibung
- Klassifizierung (niedrig, mittel, hoch)
- Wer hat den IT-Sicherheitsvorfall wann gemeldet?
- Wann ist der IT-Sicherheitsvorfall aufgetreten?
- Wer war von dem IT-Sicherheitsvorfall betroffen?
- Wann wurde der IT-Sicherheitsvorfall gelöst?
- Was wurde zur Lösung des IT-Sicherheitsvorfalls unternommen?
- Was wurde unternommen, um ein erneutes Auftreten des Vorfalls in Zukunft wirksam zu verhindern?

5. Behandlung von Ausnahmen

Ausnahmen von den Regelungen dieser Richtlinie sind nur in Absprache mit der oder dem IT-Sicherheitsbeauftragten gestattet.

6. Umsetzung

Die Leitungen der Fakultäten und Einrichtungen tragen die Verantwortung für die Umsetzung dieser Richtlinie. Regelungen dieser Richtlinie, die nicht umgesetzt werden, können an die oder den CIO oder die Leitung der Universität kommuniziert werden.

7. Revision

Diese Richtlinie wird regelmäßig, jedoch mindestens einmal pro Jahr, durch den oder die IT-Sicherheitsbeauftragte/n auf ihre Aktualität und Konformität mit den IT-Sicherheitsregelungen der Universität Bielefeld überprüft.