drucken

ERFASSUNG VON IT-SICHERHEITSEREIGNISSEN

Definition **IT-Sicherheitsereignis:** Bei einem System, einem Dienst oder in einem Netzwerkbereich fand/findet ein Ereignis statt, welches darauf hindeutet, dass Aspekte der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit, Unversehrtheit der Daten bzw. Systeme) beeinträchtigt sein könnten oder dass eine getroffene IT-Sicherheitsmaßnahme fehlschlägt oder fehlgeschlagen hat.

Jede Art von Verbesserungsvorschlägen (zum Formular, zum Vorgehen etc.) sind höchst willkommen. Bitte per Mail an it-sb@uni-bayreuth.de

Datum und Uhrzeit:
(z.B. aus dem 28.2.2017 um 12:21 Uhr wird E-20170228-12:21)

E-
(jjjjmmtt-hhmm)

Ähnlich gelagertes Ereignis
(sofern bekannt, evtl. Freitext-Antwort):

Angaben zu der das IT-Sicherheitsereignis meldenden Person:

Vor- und Nachname		Organisation	
Telefonnummer		E-Mail	

I. Weitere Bearbeitende (falls nicht identisch mit der obigen Person)

Vor- und Nachname		Organisation	
Telefonnummer		E-Mail	

Vor- und Nachname		Organisation	
Telefonnummer		E-Mail	

II. Beschreibung des IT-Sicherheitsereignisses

Datum und Uhrzeit des Auftretens: (jjjjmmtt-hhmm)

Datum und Uhrzeit der Entdeckung: (jjjjmmtt-hhmm)

Beschreibung (Bitte antworten Sie, wo Ihnen dies möglich ist, so exakt wie möglich)

Was ist passiert?

Wie ist es passiert?

Warum ist es passiert?

Welche Komponenten/Netzbereiche sind betroffen?

Welche Auswirkungen bestehen?

Wurden Schwachstellen identifiziert?

III. Typ des IT-Sicherheitsereignisses

☐ **Physischer Schaden**

☐ Feuer ☐ Wasser ☐ Elektrostatik

☐ Schädliche Umgebungseinflüsse (Schadstoffe, Staub, Korrosion, Eis,…)

☐ Zerstörung von Equipment ☐ Zerstörung von Medien

☐ Diebstahl von Equipment ☐ Diebstahl von Medien

☐ Verlust von Equipment ☐ Verlust von Medien

☐ Manipulation von Equipment ☐ Manipulation von Medien ☐ Andere

Detailbeschreibung:

☐ **Ausfall der Infrastruktur**

☐ Energieversorgung ☐ Netzwerk ☐ Klimaanlage

☐ Wasserversorgung ☐ Andere

Detailbeschreibung:

☐ **Technisches Versagen**

☐ Hardwareausfall ☐ Softwarefehler ☐ Überlastung

☐ Unterbrechung der Wartung ☐ Andere

Detailbeschreibung:

☐ **Schadprogramme**

☐ Netzwerk-Wurm ☐ Trojaner ☐ Botnet

☐ gemischte Angriffe ☐ Website mit Schadcode

☐ Website die Schadcode hostet ☐ Andere

Detailbeschreibung:

☐ **Technischer Angriff**

☐ Scannen des Netzwerks ☐ Login-Versuche ☐ Denial of Service (DoS)

☐ Ausnutzen einer Schwachstelle ☐ Ausnutzen einer Backdoor

☐ Andere

Detailbeschreibung:

☐ **Kompromittierung von Funktionen**

☐ Missbrauch von Rechten ☐ Fälschen von Rechten ☐ Fehlbedienung

☐ Verletzung personeller Verfügbarkeit ☐ Andere

Detailbeschreibung:

☐ **Kompromittierung von Informationen**

☐ Abhören ☐ Spionage ☐ Offenlegung

☐ Social Engineering ☐ Netzwerk Phishing ☐ Datendiebstahl

☐ Datenverlust ☐ Datenfälschung ☐ Datenirrtum

☐ Datenflussanalyse ☐ Positionsortung ☐ Andere

Detailbeschreibung:

☐ **Verbreitung unerwünschter Inhalte**

☐ Illegale Inhalte ☐ Panik-Inhalte (Hoax) ☐ Böswillige Inhalte

☐ Beleidigende Inhalte ☐ Andere

Detailbeschreibung:

☐ **Unbekannt**

Sofern das Sicherheitsereignis noch nicht klassifiziert werden kann, kreuzen Sie "Unbekannt“ an und beschreiben Sie soweit möglich den Typ des IT-Sicherheitsereignisses:

Detailbeschreibung:

IV. Betroffene Gegenstände

Betroffene Komponenten/Netzbereiche

Informationen/Daten

Hardware

Software

Kommunikation

Dokumentation

Dienste (z.B. E-Mail)

Personen

Ergänzende Bemerkungen

V. Auswirkungen des IT-Sicherheitsereignisses

Sofern zutreffend, kreuzen Sie untenstehende Kategorien an und gewichten Sie die folgenden Auswirkungen auf einer Skala von 1 bis 10 (1 = gering, 10 = massiv).

	Gewichtung (Skala 1-10)	Auswirkung	(Kosten) optional
☐ Verlust der Vertraulichkeit			
☐ Verlust der Integrität			
☐ Verlust der Verfügbarkeit			
☐ Verletzung von Nachweispflichten			
☐ Zerstörung			

VI. Behandlung des IT-Sicherheitsereignisses

Beteiligte Personen/Täter (falls bekannt)

☐ Person ☐ Gesetzlich berechtigte Organisation

☐ Organisierte Gruppe ☐ Unfall ☐ kein Vorsatz

Beschreibung der Täter (falls bekannt)

Tatsächliches oder vermutetes Motiv

☐ Kriminelle/finanzielle Energie ☐ Zeitvertreib/Hacking

☐ Politisch motiviert/Terror ☐ Rache ☐ Anderes

Detailbeschreibung:

Detailbeschreibung:

Realisierte Aktionen zur Lösung des Ereignisses

Offene Aktionen zur Lösung des Ereignisses

Ergebnis nach Abschluss der offenen Aktionen und evtl. weitere geplante Aktionen zur Lösung des Ereignisses

Informierte Personen

☐ IT-Servicezentrum intern (Namen angeben)

☐ Leiter IT-Servicezentrum

☐ IT-Verantwortlicher

☐ Melder des Ereignisses

☐ Hochschulleitung

☐ IT-Sicherheitsbeauftragte

☐ Lehrstuhlinhaber

☐ Chief Information Officer

Informierte Personen/Gruppen außerhalb der Organisation

☐ Polizei

☐ Weitere (z. B. Regulierungs-/Aufsichtsbehörden, externes DFN-Cert etc.))

VII. Zusammenfassende Bewertung des IT-Sicherheitsereignisses

Skala (1 -10, 1 = geringe Bedeutung , 10 = hohe Bedeutung

Skala :

Begründung der vorgenommenen Bewertung

Aufgrund Ihrer Erfahrungen mit dem IT-Sicherheitsereignis, was schlagen Sie vor, um zukünftig IT-sicherheitstechnische Verbesserungen zu erzielen? D.h. was lässt sich alles verbessern?

VIII. Unterschriften der involvierten Personen

Unterschriften (auch digital)

Autor	**Prüfer**	**Prüfer**
Name	Name	Name
_____	_____	_____
Rolle	Rolle	Rolle
_____	_____	_____
Datum	Datum	Datum
_____	_____	_____
Unterschrift	Unterschrift	Unterschrift
_____	_____	_____

Ist der Fall abgeschlossen? ☐ Ja ☐ Nein

Falls ja: Dauer des Ereignisses in Tagen/Stunden/Minuten

Bitte dieses Dokument unter Wahrung der Vertraulichkeit elektronisch oder in Papierform der IT-Sicherheitsbeauftragten Dr. Heidrun Benda, IT-Servicezentrum (it-sb@uni-bayreuth.de) zusenden.

Stand: Version 1.3 vom 01.03.2017