Technische Universität Berlin

Richtlinie zur Meldung von IT-Sicherheitsvorfällen

Version 2.2

1. Einleitung/Präambel

Zur Einhaltung und Sicherstellung des Erreichens der Ziele der IT-Sicherheitsrichtlinie ist es notwendig deren Wirkung und eventuelle Schwachstellen zu überwachen. Aus diesem Grund wird für die TU Berlin ein **zentralisiertes Meldewesen für Schwachstellen und IT-Sicherheitsrelevante Vorfälle** etabliert. Die Meldung der Vorfälle dient der Qualitätssicherung und der Einschätzung und Abwehr möglicher Gefahren für die TU Berlin, so dass eine angemessene und unmittelbare Reaktion und Umsetzung von Maßnahmen zur Schadensabwehr, -begrenzung und -beseitigung ermöglicht werden. Dadurch sollen Schäden minimiert und weitere Gefahren abgewendet werden.

2. Geltungsbereich

Diese Richtlinie gilt für alle Einrichtungen der TU Berlin, alle Mitglieder*innen und alle von IT-Systemen betroffenen Personen.

3. Meldung: Wege und Vertraulichkeit

Alle IT-sicherheitsrelevanten Vorfälle und Schwachstellen von IT-Systemen müssen unverzüglich per E-Mail an cert@tu-berlin.de gemeldet werden.

Alternativ steht Ihnen auch die ZECM-Hotline unter +49-30-314-28000 zur Verfügung.

Falls personenbezogene Daten betroffen sind oder sein könnten, beachten Sie bitte **zusätzlich** das Rundschreiben zu Datenschutzvorfällen.

Die Meldungen an das Security-Team werden vertraulich behandelt. Nur ein sehr kleiner Personenkreis innerhalb der TU Berlin hat direkten Zugriff auf die Meldungen. Davon abgeleitete Maßnahmen werden, soweit rechtlich möglich, ohne Nennung der meldenden Einheit/Person durchgeführt. Auch für Statistiken und Berichte wird diese Vertraulichkeit beibehalten.

4. Definition: IT-Sicherheitsvorfälle und -Schwachstellen

IT-Sicherheitsrelevante Vorfälle oder Schwachstellen sind Ereignisse und Umstände, die eines oder mehrere der in der IT-Sicherheitsleitlinie festgelegten **Schutzziele der IT-Sicherheit der TU Berlin verletzen oder gefährden:**

- die **Verfügbarkeit** der IT-Systeme und Daten,
- die **Vertraulichkeit** der Daten,
- der **Schutz vor unautorisiertem Zugriff**,
- die **Integrität der Daten**,
- die **Einhaltung einschlägiger Gesetze und sonstiger rechtlicher Bestimmungen** und
- das damit verbundene **Ansehen der TU Berlin in der Öffentlichkeit.**

Beispiele für IT-sicherheitsrelevante Vorfälle und Schwachstellen sind u.a.:

- Verlust oder Diebstahl von elektronischen Geräten, auf denen Daten der TU Berlin gespeichert sind,
- Einbruch von Hackern in IT-Systeme der TU Berlin,
- Befall oder Verbreitung von Schadsoftware durch an der TU Berlin betriebene IT-Systeme,
- IT-Systeme, die zur Verbreitung von Spam-E-Mails oder anderen unerwünschten Kommunikationen beitragen,
- ausgespähte, weitergegebene oder bekanntgewordene Zugangsdaten zu IT-Systemen der TU Berlin,
- sicherheitskritische Schwachstellen bei im Einsatz befindlichen IT-Geräten und IT-Systemen.

5. Inkrafttreten

Diese Sicherheitsrichtlinie tritt mit Beschluss des CIO der TU Berlin und mit Ihrer Veröffentlichung als Rundschreiben in Kraft.