Technische Universität Berlin

Der Präsident

R U N D S C H R E I B E N

☒ ALLE (Prof., WM, SM, Tut)

Bearbeiter/in:
Herr Prof. Dr. Kao

Stellenzeichen / Tel.
EN 50

Datum:
10.12.2019

Schlagwort :

Richtlinie zur Meldung von IT-Sicherheitsvorfällen

Gruppe
H

Dieses Rundschreiben

ersetzt: Rdschr. zur Meldung von IT-Sicherheitsvorfällen vom 02.08.2016

see English version below
convenience translation – not legally binding
pursuant to the decision of the Executive Board of 01.06.2018

Richtlinie zur Meldung von IT-Sicherheitsvorfällen

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.

Guidelines for Reporting IT Security Issues

1. Introduction

It is necessary to monitor the impact of the University's IT security guidelines and identify any possible shortcomings to ensure that their goals are met and their measures complied with. TU Berlin has consequently established **a central service for reporting IT security incidents and issues.** This helps improve quality assurance, evaluate possible threats for TU Berlin, take appropriate and prompt action and implement measures to protect against, limit and rectify any damage caused. This will minimize damage and prevent future risks.

2. Scope

These reporting guidelines apply to all departments and units at TU Berlin, all members of staff and students as well as anyone using or affected by the IT systems.

3. Reporting: procedures and confidentiality

All IT security system incidents and issues must be reported immediately by email to cert@tu-berlin.de.

Alternatively, you can contact the ZECM hotline at +49-30-314-28000.

Please also refer to the circular relating to data protection incidents in cases where personal data has been or might be affected.

All incidents reported to the security team will be treated in the strictest confidence. Only a very small number of people at TU Berlin have access to incident reports. Measures in response to reported incidents shall, as far as legislation permits, be introduced without mention of the person or unit reporting the incident. Strict confidentiality also applies to statistics and reports.

4. Definition: IT security incidents and issues

IT security incidents and issues refer to events or situations which **infringe or place at risk one or more of the following protective goals for IT security at TU Berlin** as established in the IT security guidelines:

- **Availability** of IT systems and data
- **Confidentiality** of data
- **Protection against unauthorized access**
- **Integrity of data**
- **Compliance with relevant laws and other legal provisions**
- **TU Berlin's public reputation**

Examples of IT security incidents and issues include:

- Loss or theft of electronic devices on which TU data has been stored
- Hacking of TU Berlin IT systems
- Infestation or distribution of malware by IT systems operated at TU Berlin
- IT systems which enable the distribution of spam emails or other unsolicited forms of communication
- Access data for TU Berlin IT systems which have been tracked, passed on or made known to others
- Security-critical weaknesses in IT equipment and IT systems in use

5. Commencement

These guidelines shall take effect upon the decision of the CIO of TU Berlin and upon their publication as a circular.