Nr. 41 | 2019
13. November 2019

Amtliche Bekanntmachungen

der Heinrich-Heine-Universität Düsseldorf

INHALT SEITE

Herausgeber
Rektorin der Heinrich-Heine-Universität Düsseldorf
Universitätsstraße 1 · 40225 Düsseldorf · www.hhu.de

Redaktion
Stabsstelle Justitiariat · Gebäude 16.11
Telefon 0211 81-11383 · justitiariat@hhu.de

RICHTLINIE FÜR DIE IT-SICHERHEIT AN DER HEINRICH-HEINE-UNIVERSITÄT DÜSSELDORF VOM 13.11.2019

1. Ziele

(1) Für die produktive und störungsfreie Wahrnehmung der Aufgaben in Forschung, Lehre und Verwaltung an der Heinrich-Heine-Universität Düsseldorf (HHU) ist eine sichere Verarbeitung von elektronischen Daten eine wesentliche Voraussetzung.

(2) Dazu ist es erforderlich, Risiken beim Einsatz von elektronischen Informationssystemen durch geeignete Maßnahmen zu minimieren, indem die Verfügbarkeit von Systemen, Daten und Diensten gewährleistet, ihre Vertraulichkeit geschützt und ihre Integrität gesichert werden.

(3) Einschlägige Gesetze und dienstliche Erfordernisse müssen berücksichtigt werden.

(4) Die Sicherheitsmaßnahmen sollen sich am Stand der Technik orientieren.

(5) Die Sicherheitsmaßnahmen sollen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen.

(6) Schadensfälle mit hohen finanziellen oder das Ansehen der HHU schädigenden Auswirkungen müssen verhindert werden.

2. Begriffsbestimmungen

(1) Einrichtungen sind die Fakultäten, die wissenschaftlichen Einrichtungen sowie die Zentrale Einrichtungen der Universität.

(2) IT-Systeme sind Datenverarbeitungsanlagen, Kommunikationssysteme und sonstige Einrichtungen zur rechnergestützten Informationsverarbeitung physikalischer oder virtueller Natur.

(3) Mobile Geräte im Sinne dieser Richtlinie sind tragbare IT-Systeme, die ortsungebunden zur Sprach- und Datenkommunikation eingesetzt werden können und über WLAN oder LAN mit dem Netzwerk der HHU verbunden sind.

(4) Der Begriff der Netze in dieser Richtlinie umfasst sowohl die „statischen Netze“, an die nicht mobile Geräte angeschlossen sind, als auch die „dynamischen Netze“ mit mobilen Nutzerinnen

und Nutzern. Weiterhin gehören dazu auch alle Netze in den Einrichtungen mit einer Verbindung zum HHU-Netz.

(5) Nutzerinnen und Nutzer sind Personen gemäß der IT- Benutzungsordnung der Heinrich-Heine-Universität Düsseldorf, die IT-Systeme im Rahmen des Geltungsbereichs dieser Richtlinie verwenden.

(6) Administratorinnen oder Administratoren sind Nutzerinnen und Nutzer, die IT-Dienste oder IT-Systeme verwalten, z.B. das selbstgenutzte IT-System oder die von anderen genutzten IT-Systeme.

(7) Schützenswerte Daten sind personenbezogene Daten im Sinne des Datenschutzrechts sowie solche Informationen, deren Bekanntwerden der Universität oder Dritten Schaden zufügen könnte.

3. Geltungsbereich

(1) Die Regelungen dieser Richtlinie gelten für Mitglieder, Angehörige und Gäste der HHU.

(2) Sie gelten für Netze und IT-Systeme auf dem Campus und die Nutzung von externen Ressourcen.

4. Verantwortlichkeiten

(1) Die Gesamtverantwortung für die IT-Sicherheit liegt bei der Hochschulleitung der Heinrich-Heine-Universität Düsseldorf.

(2) Die Verantwortung für die IT-Sicherheit in den Einrichtungen liegt bei deren Leiterinnen und Leitern. Diese müssen die IT-Sicherheit in jedem Geschäftsprozess berücksichtigen. Werden Aufgaben, die ihnen nach dieser Richtlinie obliegen, auf andere Mitarbeiterinnen oder Mitarbeiter übertragen, so ist dies unter Namensnennung zu dokumentieren. Die Verantwortlichen in den Einrichtungen sind verpflichtet, für jedes vernetzte IT-System die dienstlichen Kontaktdaten (Name, dienstliche Adresse, Telefonnummer und E-Mail-Adresse der Nutzerin/des Nutzers) oder die Uni-Kennung zu erfassen. Auch bei Systemen, die von mehreren Anwenderinnen und Anwendern genutzt werden, müssen diese Daten unter Berücksichtigung von Vorgaben durch den Datenschutz erfasst werden, z.B. durch die Protokollierung der Anmeldeaktivitäten an dem Gerät. Diese Daten sind dem ZIM bei Bedarf – z.B. im Falle einer Störung – mitzuteilen. Das ZIM kann das betreffende System im Schadensfall erforderlichenfalls vom Datennetz trennen.

(3) Bei Systemen, an denen nur vordefinierte Dienste genutzt werden können (z.B. die Bibliotheksdienste durch anonyme Benutzerinnen und Benutzer) tragen die Administratorinnen und Administratoren der Systeme die Verantwortung im Sinne dieser Richtlinie.

(4) IT-Dienste und deren Zuständigkeiten müssen dem ZIM über die bereitgestellten technischen Schnittstellen gemeldet werden.

(5) Die Verwaltung und Zuordnung von IP-Adressen aus dem öffentlichen IP-Adressraum der HHU obliegt dem ZIM.

(6) Die Leiterinnen und Leiter der Einrichtungen sind verpflichtet, zusammen mit dem ZIM die Verantwortlichkeiten für den Betrieb der IT-Systeme festzulegen und ggf. Abgrenzungen vorzunehmen.

(7) Die Aufgaben der bzw. des IT-Sicherheitsbeauftragten sind im IKM-Versorgungskonzept definiert.

(8) Gemäß dem IKM-Versorgungskonzept wird durch die KIM der HHU eine Arbeitsgruppe „IT-Sicherheit und Datenschutz“ eingesetzt, an der sich die Einrichtungen beteiligen können. Diese Arbeitsgruppe soll Strategien und Maßnahmen zur IT-Sicherheit an der HHU erarbeiten und kommunizieren. Sie wählt eine Leitung aus ihrer Mitte.

(9) Weitergehende Informationen zu dieser Richtlinie werden von der IT-Sicherheitsbeauftragten/dem IT-Sicherheitsbeauftragten innerhalb der HHU veröffentlicht.

(10) Die oder der CIO kann bei Fragen zur Auslegung dieser Richtlinie und bei strittigen Fragen konsultiert werden.

5. Feststellung und Umsetzung der Sicherheitsanforderungen

(1) Für alle IT-Systeme im Geltungsbereich dieser Richtlinie müssen die IT-Sicherheitsanforderungen festgelegt werden. Dies muss durch die Verantwortlichen in den Einrichtungen mit Unterstützung der Arbeitsgruppe „IT-Sicherheit und Datenschutz“ erfolgen. Hierzu werden Schutzbedarfsklassen festgelegt, in die die IT-Systeme eingeordnet werden müssen. Diese Aufgabe obliegt der Leiterin/dem Leiter der Einrichtung, in der das System betrieben wird. Das ZIM und die Arbeitsgruppe „IT-Sicherheit und Datenschutz“ bieten hierzu ihre Unterstützung an.

(2) Die notwendige Sensibilisierung für IT-Sicherheitsrisiken obliegt der Leiterin/dem Leiter der Einrichtung, in der das System betrieben wird. Bei der Durchführung solcher Maßnahmen unterstützt das ZIM und die Arbeitsgruppe „IT-Sicherheit und Datenschutz".
(3) In Abhängigkeit von den IT-Sicherheitsanforderungen der IT-Systeme sind von den Verantwortlichen technische und organisatorische Maßnahmen zu ergreifen, um das notwendige Sicherheitsniveau zu erreichen.

6. Organisatorische und technische Regelungen

6.1 Allgemeine Anforderungen an die Nutzung von IT-Systemen im HHU-Netz

(1) Alle Nutzerinnen und Nutzer des Geltungsbereichs sind angehalten, verantwortungsbewusst mit der IT umzugehen unter Beachtung von IT-Sicherheitsvorgaben dieser Richtlinie und ergänzender Richtlinien.

(2) Werden Sicherheitsverstöße oder gravierende Sicherheitslücken im HHU-Netz vermutet, so sind diese dem CERT (Computer Emergency Response Team, cert@hhu.de) oder der bzw. dem CIO der HHU (cio@hhu.de) zu melden. Diese treffen geeignete Maßnahmen, um die gemeldeten Vorfälle zu verfolgen und betroffene Nutzerinnen und Nutzer zu informieren.

(3) Vermutete Schwachstellen dürfen nur mit ausdrücklicher Zustimmung einer der beiden in (2) genannten Instanzen genauer exploriert werden. Nicht autorisierte Sicherheitsüberprüfungen, Portscans oder Versuche zur Überwindung von Sicherheitsmaßnahmen bei IT-Systemen der HHU sind grundsätzlich nicht zulässig.

(4) Nutzerinnen und Nutzer von mobilen Geräten müssen sich vor der Nutzung am Netzwerk authentifizieren.

(5) Für Netze, die über ein lokal administriertes Gateway mit den Netzen der HHU verbunden sind und dauerhaft betrieben werden, muss die Administratorin bzw. der Administrator dem ZIM benannt werden. Sie bzw. er muss dem ZIM die verwendeten IP-Adressen mitteilen.

6.2 Allgemeine Anforderungen an den Betrieb von IT-Systemen im HHU-Netz

(1) Alle Geräte und die Kommunikation zwischen ihnen sind auf dem neuesten Stand der Technik zu halten und mit geeigneten Maßnahmen vor unbefugten Zugriffen und Schadprogrammen zu schützen – z.B. durch Virenscanner, lokale Firewalls oder Verschlüsselungsverfahren.

(2) Die Administratorinnen und Administratoren der IT-Systeme müssen eine regelmäßige Überprüfung der Schutzmaßnahmen durchführen.

(3) Sicherheitsrelevante Korrekturen müssen zeitnah umgesetzt werden.

6.3 Fernzugriff auf das interne Netz

Der Zugriff auf IT-Systeme der HHU aus unsicheren Netzen darf nur über gesicherte Protokolle erfolgen. Im Regelfall wird dafür der VPN-Dienst des ZIM genutzt. Ausnahmen zu dieser Regelung sind mit dem ZIM abzusprechen.

7. Inkrafttreten

Diese Richtlinie für IT-Sicherheit tritt am Tag nach ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Universität in Kraft. Gleichzeitig tritt das IT-Sicherheitskonzept vom 14. Februar 2017 außer Kraft.

Ausgefertigt aufgrund des Rektoratsbeschlusses vom 7.11.2019.

Düsseldorf, den 13.11.2019

Die Rektorin
der Heinrich-Heine-Universität
Düsseldorf

Anja Steinbeck
(Univ.-Prof. Dr. iur.)

Anlagen:

1. Erläuterung der Vorgehensweise zur Erstellung einer Schutzbedarfsanalyse

Anlage: Schutzbedarfsanalyse in Anlehnung an den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik[1]

Die Leiterinnen und Leiter der Einrichtungen sind dafür verantwortlich, Schutzmaßnahmen für ihre IT-Systeme, die darauf laufenden Anwendungen und die von diesen Anwendungen verwendeten Daten zu ergreifen. Die Schutzmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der Systeme, der Anwendungen und der Daten stehen.

Um angemessene Schutzmaßnahmen festzulegen, muss erst der Schutzbedarf festgestellt werden. Dafür hat sich die folgende Vorgehensweise als hilfreich erwiesen:

1. Definieren Sie möglichst alle relevanten IT-bezogenen Geschäftsprozesse, Aufgaben, Forschungsvorhaben etc. in Ihrem Bereich (z.B. die Bewertung von Klausuren und die Mitteilung der Ergebnisse an die Studierenden, die Durchführung von Beschaffungen, die Erstellung eines Forschungsberichtes oder das Erheben von Forschungsdaten).

2. Bestimmen Sie dafür die folgenden Informationen:

   - Wie lange darf dieser Prozess/diese Aufgabe maximal ausfallen? Der somit bestimmte Wert legt die *Anforderung an die Verfügbarkeit* fest.

   - Wie vertraulich sind diese Daten? Wie gravierend ist es, wenn eine unbefugte Person Zugriff darauf erhält? Die Antwort auf diese Fragen legt fest, die hoch die *Anforderung an die Vertraulichkeit* ausfallen muss.

   - Wie hoch ist der Schaden, wenn Daten durch Unbefugte verändert werden? Von der Antwort auf diese Frage hängt ab, wie hoch die *Anforderung an die Integrität* der Daten gestellt werden muss.

   Unter der Fragestellung „Was wäre, wenn…?“ müssen Sie sich realistische Schadensszenarien vorstellen und die zu erwartenden materiellen oder ideellen Schäden beschreiben. Hier ist Ihre persönliche Einschätzung Ausschlag gebend, denn nur Sie als Eigentümerinnen und Eigentümer der Daten können beurteilen, wie hoch der Schaden in einem bestimmten Szenario wäre.

3. Weisen Sie allen Prozessen, Aufgaben und Vorhaben als Ergebnis Ihrer Bewertung einer Schutzbedarfsklasse zu. Dabei legt die Schutzbedarfsklasse das mögliche Schadenspotential fest, welches bei Verstoß gegen Anforderungen von Verfügbarkeit, Vertraulichkeit und Integrität erreicht werden könnte. Die mit einem Prozess verarbeiteten Daten, die genutzten Anwendungen und die IT-Systeme, auf denen diese Prozesse bearbeitet werden, gehören der gleichen Schutzbedarfs-

[1] Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

klasse an wie der Prozess selber. Orientieren können Sie sich bei der Zuweisung einer Schutzbedarfsklasse an der folgenden Tabelle, die vier verschiedene Schutzbedarfsklassen vorgibt:

	Schutzbedarfsklasse			
	Geringes Schadenspotenzial	Normales Schadenspotenzial	Hohes Schadenspotenzial	Sehr hohes Schadenspotenzial
Verstoß gegen Gesetze, Vorschriften oder Verträge	Verstöße bleiben ohne Konsequenzen	Verstöße mit geringfügigen Konsequenzen (z.B. geringe Konventionalstrafen)	Verstöße mit hohen Konsequenzen (z.B. sind Prüfungsergebnisse besonders schutzbedürftige personenbezogene Daten, deren Verlust oder Bekanntwerden die Betroffenen erheblich beeinträchtigen können)	Fundamentaler Verstoß, dessen Haftungsschäden ruinös sind
Beeinträchtigung der persönlichen Unversehrtheit	Nicht möglich	Nicht möglich	Beeinträchtigung der persönlichen Unversehrtheit kann nicht gänzlich ausgeschlossen werden (z.B. wenn personenbezogene Daten wie etwa die Adresse einer Person einem »Stalker« bekannt werden)	Gravierende Beeinträchtigung der persönlichen Unversehrtheit ist möglich, es besteht Gefahr für Leib und Leben, etwa bei einem Verstoß gegen die Integrität medizinischer Daten, da bei fehlerhaften Daten eine Beeinträchtigung der persönlichen Unversehrtheit zu befürchten ist
Negative Innen- oder Außenwirkung	Keine Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten	Geringe Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten (z.B. kann ein Verlust von oder Verstoß gegen die Vertraulichkeit von Prüfungsergebnissen eine große Vertrauensbeeinträchtigung für die HHU bedeuten)	Eine landesweite Ansehens- bzw. Vertrauensbeeinträchtigung, die eventuell sogar existenzgefährdend sein kann, ist zu erwarten
Finanzielle Auswirkungen	Keine finanziellen Auswirkungen sind zu erwarten	Tolerable finanzielle Auswirkungen sind zu erwarten	Beträchtliche finanzielle Verluste sind zu erwarten, sie sind jedoch nicht existenzbedrohend sind (z.B. kann ein Verlust oder ein Verstoß gegen die Vertraulichkeit von Patentdaten zu hohen finanziellen Einbußen führen)	Existenzbedrohende finanzielle Verluste sind zu erwarten

4. Auf diesen Schutzbedarfsbetrachtungen aufbauend müssen die erforderlichen personellen, technischen, organisatorischen und infrastrukturellen Sicherheitsmaßnahmen ausgewählt werden, die zum Schutz dieser Daten erforderlich sind. Dazu kann man das BSI-Grundschutz-Kompendium heranziehen. Zentrale Komponente dieses Grundschutz-Kompendiums sind sogenannte „Bausteine“, die in zehn Schichten aufgeteilt sind und sich mit unterschiedlichsten Themen der IT-Sicherheit befassen – von IT-Sicherheitsaspekten bei der „Konzeption und Vorgehensweise (CON)“ über die „IT-Systeme (SYS)“ bis hin zu den „Anwendungen (APP)“.

Betrachtet man nun zum Beispiel den Baustein „Allgemeiner Client“, enthält dieser eine Liste von Empfehlungen, welche konkreten Sicherheitsmaßnahmen für den sicheren Betrieb eines solchen Systems umgesetzt werden sollten. Dort werden – ausgehend von der Konzeption eines Systems für den gesamten Lebenszyklus – Hinweise für umzusetzende Sicherheitsmaßnahmen gegeben: für die Beschaffung (Maßnahme „Beschaffung von Clients“), die Installation und Konfiguration (Maßnahme „Sichere Installation und Konfiguration von Clients“) bis hin zu einem sicheren Betrieb (Maßnahmen „Updates und Patches für Firmware, Betriebssystem und Anwendungen“ oder „Richtlinie zur sicheren IT-Nutzung“).

Sie müssen nun für alle von Ihnen identifizierten Prozesse bzw. Aufgaben und Vorhaben überlegen, welche der Bausteine angewandt werden müssen: Bei der Erstellung eines Forschungsberichtes müssen zum Beispiel die schützenswerten Forschungsdaten ggf. verschlüsselt über das Netzwerk übertragen werden und auf einem sicheren System gespeichert und ausgewertet werden. Der zugehörige Forschungsbericht soll ebenfalls auf einem abgesicherten Endsystem erstellt werden. Damit wären für dieses Vorhaben alle Sicherheitsmaßnahmen relevant, die u.a. in den folgenden Bausteinen aufgeführt werden: „Personal“ (Bereich *Organisation und Personal*) und „Datenschutz“ (Bereich *Konzeption und Vorgehensweisen*), „Büroarbeitsplatz“, „Allgemeines Gebäude“ (Bereich *Infrastruktur*), „Allgemeiner Client“, „Client unter Windows 8.1“ (Bereich *IT-Systeme*), „Lokale Netze“ (Bereich *Netze und Kommunikation*), „Webanwendungen“, „Webserver“ (Bereich *Anwendungen).*

Wenn Sie die in den IT-Grundschutzkatalogen angegebenen Sicherheitsmaßnahmen erfüllen, haben Sie ein Sicherheitsniveau erreicht, das den notwendigen Schutz für Daten mit normalem Schutzbedarf bietet. Für höheren Schutzbedarf sind darüber hinaus gehende Betrachtungen erforderlich. Dieses erfolgt aber erst, nachdem der IT-Grundschutz geschaffen worden ist.

Verfahrenshinweis

Es wird darauf hingewiesen, dass die Verletzung von Verfahrens- und Formvorschriften dieses Gesetzes oder des Ordnungs- oder des sonstigen autonomen Rechts der Hochschule gegen eine Ordnung der Hochschule nach Ablauf eines Jahres seit ihrer Bekanntmachung nicht mehr geltend gemacht werden kann, es sei denn,

1. die Ordnung ist nicht ordnungsgemäß bekannt gemacht worden,
2. das Rektorat hat den Beschluss des die Ordnung beschließenden Gremiums vorher beanstandet,
3. der Form- oder Verfahrensmangel ist gegenüber der Hochschule vorher gerügt und dabei die verletzte Rechtsvorschrift und die Tatsache bezeichnet worden, die den Mangel ergibt, oder
4. bei der öffentlichen Bekanntmachung der Ordnung ist auf die Rechtsfolge des Rügeausschlusses nicht hingewiesen worden. Die aufsichtsrechtlichen Befugnisse nach § 76 HG bleiben unberührt.