Leitlinie zur IT-Sicherheit an der Universität Passau

beschlossen von der Universitätsleitung am 24.02.2015

Vorbemerkung

In der IT-Strategie der Universität Passau ist unter Punkt 2.2.3 die Entwicklung und Umsetzung von Konzepten für IT-Sicherheit und Datenschutz vorgesehen.[1]

IT-Sicherheit ist ein fortlaufender Prozess, deshalb müssen entsprechende Sicherheitskonzepte ständig an veränderte Bedrohungsszenarien angepasst werden. Auf der anderen Seite können die Grundsätze (Leitlinie) für die IT-Sicherheit an der Universität Passau in kompakter und relativ statischer Form definiert werden.

Die Leitlinie bildet die Grundlage für zukünftige IT-Sicherheitsrichtlinien, die als Ergänzung bzw. Präzisierung dieser Leitlinie formuliert werden. Die Leitlinie und die darauf aufbauenden Richtlinien bilden zusammen das Regelwerk (Konzept) für IT-Sicherheit an der Universität Passau.

1 Notwendigkeit und Ziele von IT-Sicherheit

IT-Systeme bestimmen in immer größerem Ausmaß den Arbeitsalltag der Nutzerinnen und Nutzer. Anders als in früheren Zeiten sind heute die meisten IT-Systeme vernetzt. Insbesondere mit dem Internet verbundene Rechnersysteme sind einem stetig steigendem Maß an Angriffen ausgesetzt. Auch bei den Rechnern der Universität Passau ist dies zu beobachten. Da die stetige Verfügbarkeit von Rechnersystemen für die tägliche Arbeit fast unentbehrlich geworden ist, stellen versuchte oder erfolgreiche Angriffe – nicht nur aus dem Internet, sondern möglicherweise auch aus dem Intranet der Universität Passau selbst – auf IT-Systeme der Universität eine schwerwiegende Beeinträchtigung dar.

IT-Systeme werden miteinander vernetzt, um auf einfache Weise Daten zwischen ihnen austauschen zu können. Während die Systeme früher nur auf Arbeitsgruppen- oder Institutsebene vernetzt wurden, sind heutzutage durch das Internet die Rechner praktisch weltweit miteinander verbunden. Die unbestreitbaren Vorteile für die Beschäftigten und Studierenden liegen darin, dass sie auf eine große Menge von angebotenen Diensten zugreifen können, ohne den Arbeitsplatz verlassen zu müssen. Leider ist umgekehrt auch jedes vernetzte IT-System ein potentielles Angriffsziel für Cyberkriminelle ("Hacker") auf der ganzen Welt. Die Angriffsszenarien sind hierbei ständigen Veränderungen unterworfen.

Der Begriff "IT-Sicherheit" lässt sich allgemein über die fünf in Abbildung 1 dargestellten Säulen definieren. Die Gewichtung der einzelnen Säulen hängt allerdings stark von der konkreten Anwendungssituation ab.

1 http://www.uni-passau.de/it-strategie.html

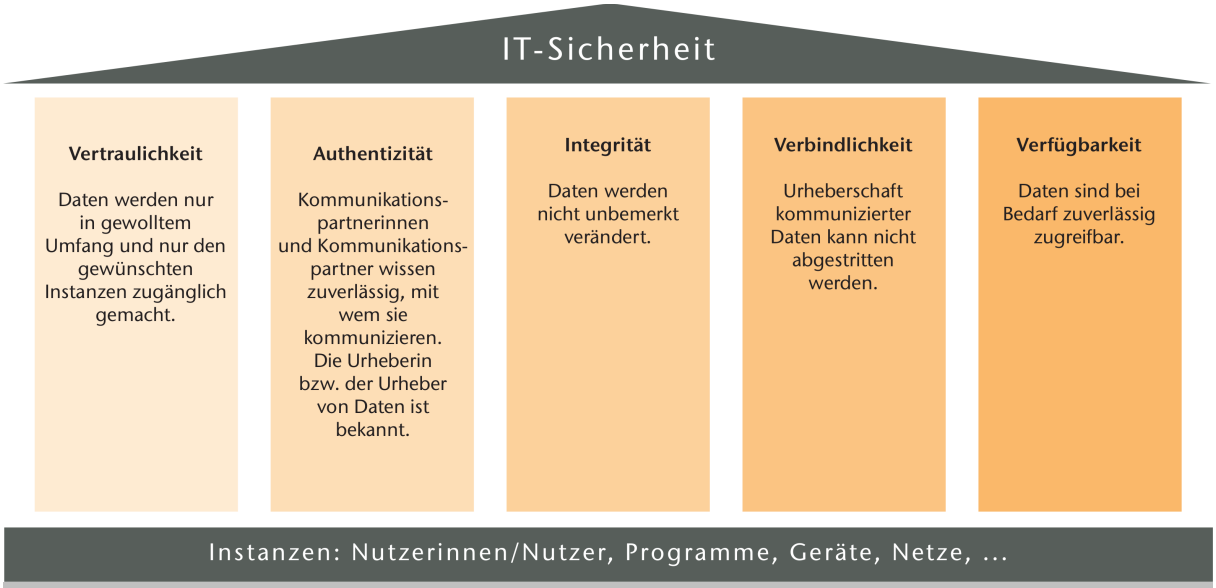

Abbildung 1: Säulen der IT-Sicherheit

Diese IT-Sicherheitsleitlinie definiert die wichtigsten Anforderungen an IT-Sicherheit für die gesamte Universität Passau. Damit wird die Grundlage für eine vertrauensvolle Nutzung von Informationstechnologie sowohl durch Universitätsangehörige als auch externe Kommunikationspartnerinnen und -partner geschaffen.

Es ist grundsätzlich sehr aufwendig bzw. gar nicht möglich, jede einzelne mit IT arbeitende Instanz zu 100% sicher zu machen. Eine konsequent umgesetzte Sicherheitsstrategie hilft aber wirkungsvoll, missbräuchliche Nutzung von IT (die im Prinzip das Resultat eines jeden Sicherheitsvorfalls sein kann) zu vermeiden.

An der Universität Passau werden insbesondere die folgenden IT-Sicherheitsziele verfolgt:

- Schutz der Netzwerkinfrastruktur und der IT-Systeme einschließlich der damit verarbeiteten Daten gegen Missbrauch oder Sabotage von innen und außen.
- Sicherstellung eines robusten, verlässlichen und sicheren Lehr-, Forschungs- und Verwaltungsbetriebs.
- Realisierung sicherer und vertrauenswürdiger Online-Dienstleistungen für Nutzerinnen und Nutzer in und außerhalb der Universität.
- Gewährleistung der Erfüllung der aus den gesetzlichen Vorgaben resultierenden Anforderungen an den Datenschutz.

Für die Erreichung dieser Ziele sind nicht nur technische, sondern auch organisatorische und personelle Maßnahmen einzuplanen und entsprechende Ressourcen zur Verfügung zu stellen.

Eine Kompromittierung von IT-Sicherheit kann die Universität sowohl im internen als auch im externen Bereich beeinträchtigen - intern etwa durch eine Beeinträchtigung der Produktivität, in der Außenwirkung beispielsweise durch temporären Ausschluss von Internetdiensten oder auch Rufschädigung. Darüber hinaus werden für die Schadensbehebung z. T. erhebliche personelle Ressourcen verbraucht.

Grundsätzlich ist bei der Gestaltung von Sicherheitsmaßnahmen so vorzugehen, das einzelne Sicherheitsvorfälle möglichst geringe Auswirkungen auf die gesamte IT-Sicherheit haben ("Minimal Impact-Strategie"). Unabdingbar hierfür ist die Einhaltung des Minimalprinzips für die Konfiguration und Nutzung von IT-Systemen:

- Zugriffsrechte für Benutzerinnen und Benutzer
- Systemrechte für die eingesetzte Software
- Zugriffe auf Dienste über das Netzwerk

sind auf die Erfüllung der jeweiligen Aufgabe bzw. die Erreichung des beabsichtigten Ziels zu beschränken.

Einer umfassenden Gewährleistung von IT-Sicherheit steht das Bedürfnis berechtigter Benutzerinnen und Benutzer gegenüber, möglichst wenige Einschränkungen in der Nutzung von IT hinnehmen zu müssen. Gerade an einer Universität, wo die Nutzungsbedürfnisse durchaus heterogen sind, ist die Durchsetzung von Sicherheitsmaßnahmen - vor allem wenn sie Einbußen beim Bedienungskomfort mit sich bringen - oft schwierig. Daher müssen IT-Sicherheitsrichtlinien versuchen, eine angemessene Balance zwischen IT-Sicherheit einerseits und "Usability" andererseits herzustellen.

Dies gilt auch deshalb, weil die Erfahrung zeigt, dass Sicherheitsmaßnahmen, die die Nutzerinnen und Nutzer zu stark in ihrer Arbeit behindern, oft umgangen werden und dann wirkungslos sind. Es ist daher oft wirkungsvoller, auf die größtmögliche Sicherheitsstufe zu verzichten, dafür aber Sicherheit in der Praxis auch gewährleisten zu können. In diesem Fall ist aber auch mit einem höheren Risiko erfolgreicher Angriffe zu rechnen.

Gefährdungen durch IT-Sicherheitsvorfälle mit straf- und zivilrechtlicher Relevanz, die sich aus einer verhältnismäßig unbeschränkten Nutzungsmöglichkeit des Internet an der Universität Passau ergeben, sind auch auf organisatorischer Ebene zu adressieren. Entsprechende Regularien müssen ggf. an anderer Stelle über Dienstvereinbarungen und/oder Nutzungsordnungen festgelegt werden.

2 Sicherheitszonen

Vernetzte IT-Systeme sind heutzutage allgegenwärtig. Für die Definition von Schutzmaßnahmen müssen verschiedene Arten von Zugriffsmöglichkeiten berücksichtigt werden:

- Physische Zugriffsmöglichkeiten sind durch den räumlichen Standort gegeben (z. B. öffentlicher oder nichtöffentlicher Bereich).
- Logische Zugriffsmöglichkeiten umfassen den Zugriff auf oder durch ein System über das Netzwerk oder auch andere Kommunikations-schnittstellen.

Je nach individuell gegebenen bzw. gewünschten physischen und logischen Zugriffsmöglichkeiten müssen Maßnahmen zum Schutz vor unautorisiertem Zugriff getroffen werden, wobei hier das im letzten Abschnitt formulierte Minimalprinzip beachtet werden muss. Die notwendigen Maßnahmen werden in einzelnen Sicherheitsrichtlinien präzisiert.

3 Geltungsbereich

Diese Leitlinie gilt für

a) alle IT-Systeme, die im erweiterten Intranet der Universität Passau betrieben werden, unabhängig davon, ob es sich um dienstliche oder private Geräte ("BYOD" - Bring Your Own Device) handelt,
b) IT-Systeme, die außerhalb des Intranets der Universität Passau auf zugangsgeschützte Dienste im Intranet der Universität Passau zugreifen,
c) die Administratoren und Nutzerinnen und Nutzer der unter a) und b) aufgeführten IT-Systeme.

Die Leitlinie und darauf aufbauende Sicherheitsrichtlinien sind für IT-Systeme mit normalem Schutzbedarf ausgelegt. Lt. BSI-Standard 100-2, Abschnitt 4.3.1, ist dieses Schutzniveau dadurch gekennzeichnet, dass "Schadensauswirkungen begrenzt und überschaubar" sind, sich also etwa wie folgt darstellen:[2]

Verstoß gegen Gesetze, Vorschriften,Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung Betroffene in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigt werden können.
Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.

2 vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.

Systeme mit hohem oder sehr hohem Schutzbedarf an der Universität benötigen ggf. zusätzliche Schutzmaßnahmen, die als Resultat einer individuellen Sicherheitsanalyse festgelegt werden müssen. Bei der Klassifikation des Schutzbedarfs, die grundsätzlich die oder der Betreibende eines IT-Systems vornehmen muss, ist im Zweifel die oder der Datenschutzbeauftragte der Universität und die oder der IT-Sicherheitsbeauftragte (siehe nächsten Abschnitt) hinzuzuziehen.

4 Sicherheitsorganisation

An der Universität Passau wird der Problemkreis "IT-Sicherheit" in die bestehende IT-Organisationsstruktur eingebunden. Zuständig ist die oder der "Beauftragte für IT-Sicherheit" (CISO, mancherorts auch als BITS bezeichnet). Die oder der CISO ist Mitglied des IT-Steuerkreises der Universität.

Die oder der CISO hat insbesondere folgende Aufgaben:

- Erarbeitung und Fortschreibung des IT-Sicherheitskonzepts, von IT-Sicherheitsrichtlinien und -regelungen,
- Beratung und Unterstützung der Universitätsleitung, der oder des CIO, des IT-Steuerkreises, der IT-Services sowie der Administratorinnen und Administratoren bei der Umsetzung von IT-Sicherheitsaufgaben,
- Koordinierung und Prüfung von IT-Sicherheitsmaßnahmen,
- Information und Sensibilisierung der Universitätsangehörigen zum Thema IT-Sicherheit, auch im Rahmen von Informationsveranstaltungen,
- Ansprechperson für alle Universitätsangehörigen im Bereich IT-Sicherheit, insbesondere bei IT-Sicherheitsvorfällen und -mängeln. Für diesen Aufgabenbereich soll eine Vertretung bei Abwesenheit benannt werden.

Aus Abbildung 2 geht hervor, dass die oder der CISO der Universität Passau die zentrale Schnittstelle für IT-Sicherheitsbelange nicht nur innerhalb der Universität, sondern auch als Vertretung nach außen ist, etwa in Kommunikation mit dem DFN-CERT, dem BSI oder weiteren (auch internationalen) Sicherheitsorganisationen.

Aus personellen Gründen gibt es an der Universität Passau kein eigenständiges Sicherheitsteam ("CERT"). Umso wichtiger ist es, dass sich alle Nutzerinnen und Nutzer der IT-Infrastruktur der Universität Passau über die Notwendigkeit und Bedeutung von IT-Sicherheit bewusst sind.

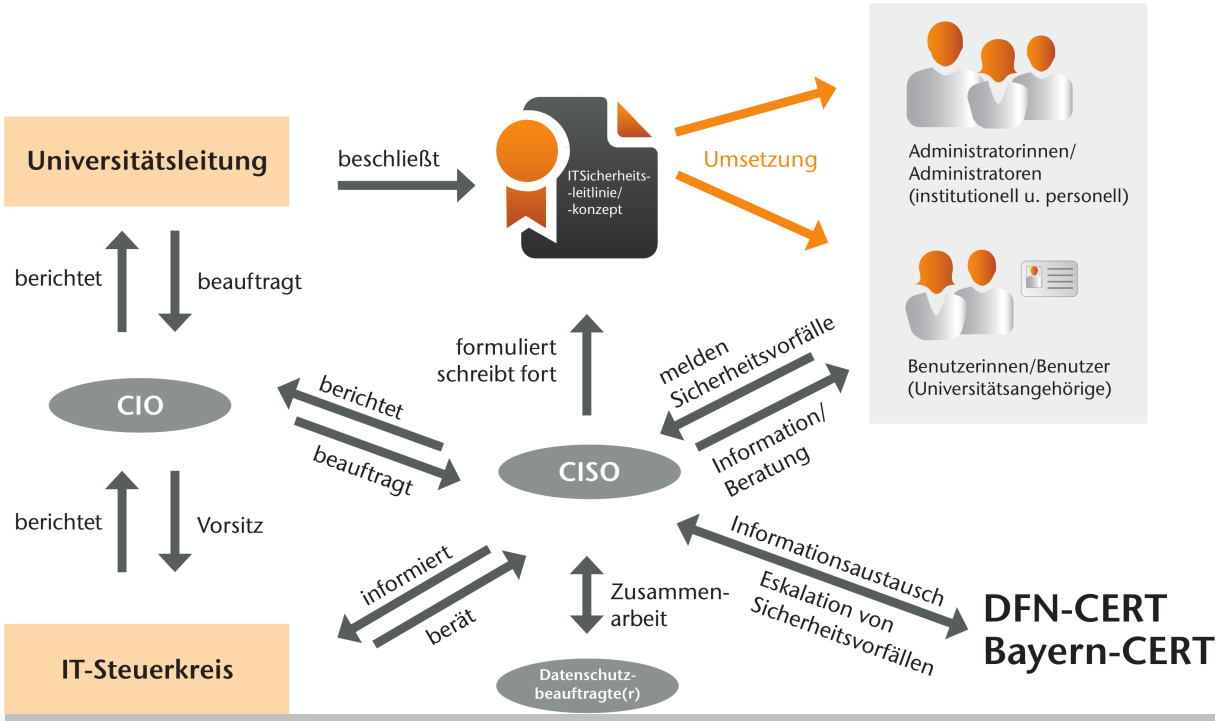

Abbildung 2: IT-Sicherheit in der Organisationsstruktur der Universität Passau

5 Verantwortlichkeiten

IT-Sicherheit funktioniert nur ganzheitlich. Damit ist es zum einen nicht getan, sich auf technische Maßnahmen zu beschränken. Oft können Probleme nicht durch Technik, sondern nur (oder zumindest: auch) durch organisatorische Maßnahmen gelöst werden. Zum anderen kann das angestrebte Sicherheitsniveau nur erreicht werden, wenn ausnahmslos alle Universitätsangehörigen und sonstigen Nutzerinnen und Nutzer der universitären IT-Infrastruktur einbezogen werden.

In Abbildung 3 ist schematisch dargestellt, welche Instanzen am Komplex "IT-Sicherheit" beteiligt sind.

Grundsätzlich lässt sich die (nicht-technische) politische, organisatorische, personelle Ebene und die rein technische Ebene unterscheiden, wobei letztere auf die nicht-technischen Ebenen durchschlägt, da die Technik ja von Menschen konzeptioniert und bedient werden muss.

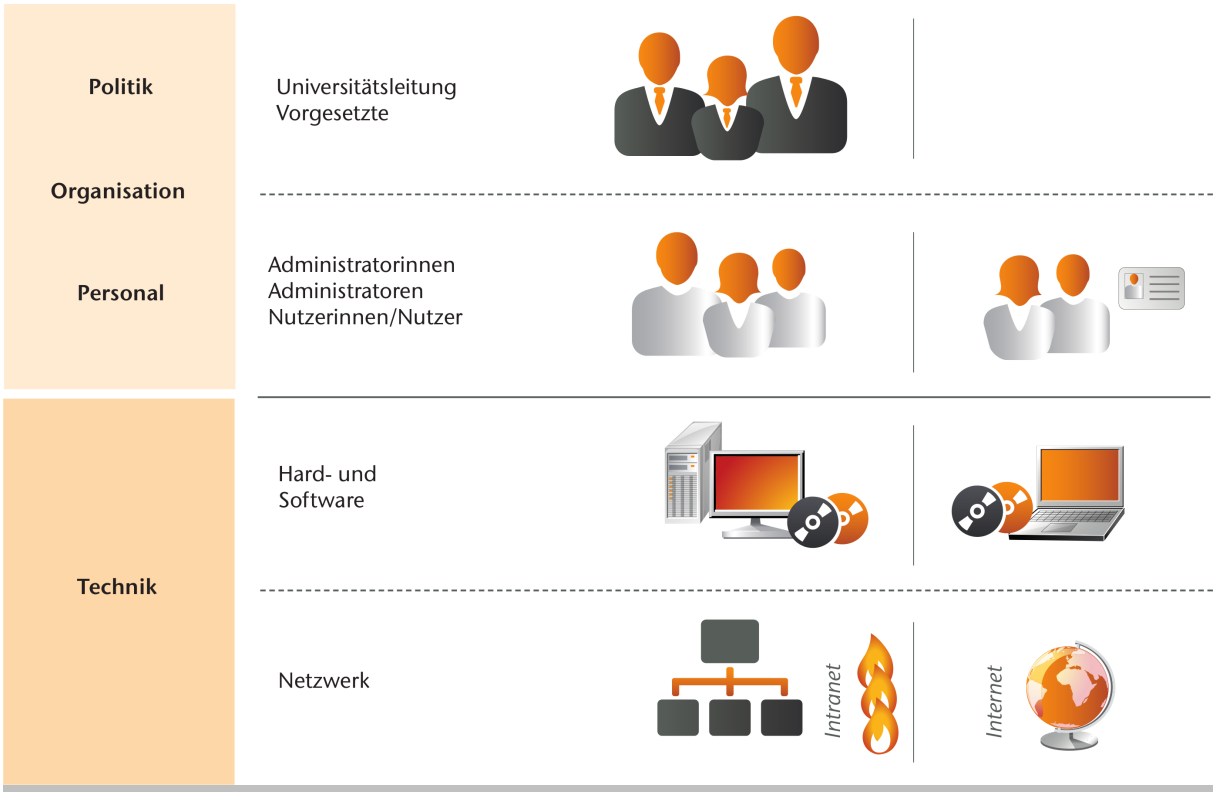

Abbildung 3: An IT-Sicherheit beteiligte Instanzen

a) Die **Universitätsleitung** bzw. die oder der von ihr eingesetzte **CIO** hat die Gesamtverantwortung für IT-Sicherheit und unterstützt aktiv ihre Umsetzung, u. a. auch indem die für IT-Sicherheit zuständigen Beschäftigten mit den erforderlichen Kompetenzen und Ressourcen ausgestattet werden.

b) Die **Vorgesetzten** sind verantwortlich für die Umsetzung von IT-Sicherheit in ihrem Verantwortungsbereich. Sie weisen insbesondere die Mitarbeiterinnen und Mitarbeiter ihres Bereichs auf das geltende Regelwerk für IT-Sicherheit und seine Verbindlichkeit hin.

c) Die **Administratorinnen** und **Administratoren** von IT-Systemen sorgen als technische Verantwortliche in ihrem Zuständigkeitsbereich für die praktische Realisierung. Dies beinhaltet insbesondere, dass sich die Administratorinnen und Administratoren laufend proaktiv über bekannt gewordene Sicherheitslücken und Schwachstellen der auf ihren Systemen eingesetzten Software informieren und ggf. zeitnah Fehlerkorrekturen ("Patches") einspielen oder Workaround-Prozeduren installieren.

d) Auch (End-)**Nutzerinnen** und (End-)**Nutzer** sind für die Aufrechterhaltung der IT-Sicherheit an ihren Arbeitsplätzen und in ihren Umgebungen verantwortlich. Dazu gehört die operative Umsetzung der Sicherheitsleitlinie sowie nachgeordneter Richtlinien in ihren Bereichen.

e) Das **Netzwerk** bildet als zentrale Kommunikations-Infrastruktur die Basis jeglicher IT-Sicherheit. Daher ist es unabdingbar, dass der Betrieb des Netzwerks durch eine zentrale IT-Serviceeinrichtung erfolgt.

Bei Differenzen über die Umsetzung dieser Leitlinie und der darauf aufbauenden Richtlinien wird die oder der CIO über den konkreten Vorgang informiert. Die oder der CIO trifft dann im Benehmen mit der oder dem CISO eine Entscheidung in der strittigen Sache.

6 Verfahren bei Sicherheitsvorfällen

Ein **Sicherheitsvorfall** ist eine im Geltungsbereich dieser Leitlinie vermutete oder tatsächlich eingetretene Gefährdung einer der in Abschnitt 1 aufgeführten Säulen für IT-Sicherheit.

Ereignete sich der Vorfall an einer Einrichtung, sind grundsätzlich die betroffenen Benutzerinnen und Benutzer innerhalb der Einrichtung unverzüglich von den an der Einrichtung Verantwortlichen über den Vorfall in Kenntnis zu setzen.

Die Administratorinnen und Administratoren bzw. Nutzerinnen und Nutzer der betreffenden IT-Systeme haben dafür Sorge zu tragen, dass nach Feststellung des Vorfalls keine weiteren (neuen) Schadensauswirkungen entstehen. Im Normalfall bedeutet das, dass die kompromittierten Systeme vom Produktivnetz genommen und einer eingehenden Analyse unterzogen werden müssen. Vor Wiederinbetriebnahme muss die Ursache des Sicherheitsvorfalls durch geeignete Maßnahmen beseitigt werden.

Aus Gründen der Beweissicherung wird vor einer Modifikation des kompromittierten Systems die Anfertigung einer Image-Backups empfohlen. Dieses Backup sollte mindestens für drei Monate aufbewahrt werden.

Wenn eine Schadensauswirkung

(1) auch außerhalb der betroffenen Einrichtung nicht ausgeschlossen werden kann oder
(2) der Vorfall ursächlich keiner Einrichtung zugeordnet werden kann,

muss die oder der CISO unverzüglich nach Feststellung des Vorfalls informiert werden.

Die Verantwortung für die korrekte Meldung von Sicherheitsvorfällen liegt im Falle von (1) beim der Leitung der betroffenen Einrichtung, im Falle von (2) beim der Leitung der Einrichtung, die den Sicherheitsvorfall festgestellt hat.

Die oder der CISO

- dokumentiert aufgrund der ihr oder ihm gegebenen Informationen den Vorfall,
- nimmt eine Einschätzung des Schweregrades vor,
- informiert ggf. die Betroffenen über die Problematik und berät sie auf Wunsch bei Einleitung geeigneter Maßnahmen,

- setzt wenn notwendig die Datenschutzbeauftragte oder den Datenschutzbeauftragten der Universität von dem Vorfall und seinen möglichen Auswirkungen in Kenntnis,
- empfiehlt ggf. die Einbeziehung weiterer Stellen (z. B. DFN-CERT, Bayern-CERT, Ermittlungsbehörden) und spezialisierter Gruppen (z. B. professionelle IT-Forensikerinnen und Forensiker),
- schätzt die Notwendigkeit ein, einen weiteren Nutzerkreis außerhalb der betroffenen Einrichtung zu informieren.
- gibt Empfehlungen für eine Wiederherstellung bzw. Verbesserung der IT-Sicherheit,
- informiert laufend die oder den CIO über den Sicherheitsvorfall und die unternommenen Schritte.

Folgende Informationen sind für eine Dokumentation und Einschätzung eines Sicherheitsvorfalls essentiell:

- Welche Systeme wurden kompromittiert (Hostnamen, IP-Adressen)? Betriebssystem, Patchstand, eingesetzte Software!
- Wann (Datum) wurde der Sicherheitsvorfall bemerkt? Wann ereignete sich der Vorfall vermutlich (erstmals)?
- Wer hat den Vorfall bemerkt? Wer ist für das kompromittierte System verantwortlich? Wer ist Ansprechperson für die oder den CISO und die ggf. einzubeziehenden Stellen?
- Art und Ursache des Vorfalls, soweit identifizierbar.
- Art der getroffenen Maßnahmen zur Beseitigung der Ursache des Vorfalls.

Zur Schadensbegrenzung bei Gefahren für die IT-Sicherheit können Nutzerinnen und Nutzer temporär von der Nutzung des Netzwerks und/oder IT-Diensten ausgeschlossen werden. Dies umfasst bei entsprechend schwerwiegenden Gefahren auch die Trennung von Endgeräten oder Subnetzen vom Intranet und Internet.

Bei wichtigen Sicherheitsvorfällen muss die Universitätsleitung von CIO oder CISO informiert werden.

7 Maßnahmen bei Sicherheitsmängeln

Ein **Sicherheitsmangel** ist eine Schwachstelle in einem IT-Dienst oder IT-Verfahren, die zu einem Sicherheitsvorfall nach Punkt 6 führen kann. Entdeckte Sicherheitsmängel sollten der oder dem CISO unverzüglich zur Kenntnis gebracht werden.

Die oder der CISO wird die Verantwortlichen über die Problematik in Kenntnis setzen und sie auf Wunsch bei der Abstellung des Mangels beraten. Wird der Sicherheitsmangel nicht in absehbarer Zeit beseitigt, obwohl dies mit vertretbarem Aufwand möglich wäre, informiert die oder der CISO die oder den CIO, welcher dann über das weitere Vorgehen entscheidet.

Besteht Anlass zu der Annahme, dass ein Sicherheitsmangel mehrere Bereiche innerhalb der Universität betrifft, ist die oder der CISO zur Einleitung von Maßnahmen berechtigt, die eine genauere Lokalisierung des Mangels ermöglichen.

8 Präventionsmanagement

Die oder der CISO kann die Durchführung von sog. Schwachstellenanalysen (engl. "vulnerability assessments"), also das (automatische) Aufspüren von Schwachstellen in den an der Universität betriebenen IT-Systemen, veranlassen, wenn aufgrund von Sicherheitsmeldungen von anerkannten Organisationen wie DFN-CERT, CERT-Bund, Bayern-CERT, NIST-NVD bzw. Hard- oder Softwareherstellern Grund zu der Annahme besteht, dass IT-Systeme an der Universität Passau von den Schwachstellen betroffen sein könnten.

Soweit durch eine Schwachstellenanalyse die Betriebssicherheit von IT-Systemen beeinträchtigt oder datenschutzrechtliche Bereiche berührt werden könnten, wird die oder der CISO zuvor den Umfang der Maßnahme mit CIO bzw. der oder dem Datenschutzbeauftragten abstimmen.

9 Inkrafttreten

Diese Leitlinie wird von der Universitätsleitung verabschiedet. Sie tritt am Tag nach ihrer Bekanntmachung im Virtuellen Amtsblatt der Universität in Kraft.