Initiative des AKIF: AG IT-Sicherheit nach der EU-DSGVO

Prof. Dr. Rainer W. Gerling & Dr. Ulrich Pordesch
Sprecherkreis
AKIF

Was ist der AKIF?

- Die Allianz der Wissenschaftsorganisationen gründet am 16.2.2008 den Arbeitskreis Informationssicherheit der (außeruniversitären) deutschen Forschungseinrichtungen (AKIF)
- Konzept eines Arbeitskreises der IT-Sicherheitsbeauftragten der deutschen Forschungseinrichtungen
  - Prof. Dr. Rainer W. Gerling, Max-Planck-Gesellschaft
  - Uwe Gorschütz, Deutsches Zentrum für Luft und Raumfahrt
  - Dr. Ulrich Pordesch, Fraunhofer Gesellschaft
- Mitglieder sind um die 80 außeruniversitäre Forschungseinrichtungen
  - Über die HRK auch (ca. 40) Hochschulen
- Ziel des Arbeitskreises ist die Erhöhung der IT-Sicherheit in den Forschungseinrichtungen.
- Einen Ausgleich zwischen der Forschungsfreiheit auf der einen Seite und den zunehmenden Restriktionen durch Sicherheitsanforderungen auf der anderen Seite zu schaffen.

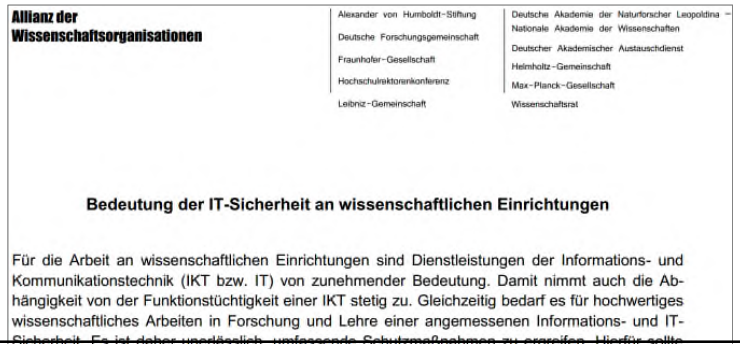
Allianz der Wissenschaftsorganisationen

- Wissenschaftspolitik
- Forschungsförderung
- strukturelle Weiterentwicklung des Wissenschaftssystems
- 2017: HGF

Arbeit des AKIF

- Am 11.6.2014 Bericht an die Allianz über die Cyber-Bedrohungen der Wissenschaft
- Am 18.9.2014 Strategie-Papier in die Allianz eingebracht

- Informationen zur Cyberabwehr aus Sicherheitsbehörden
- Tagungen zu aktuellem Thema
- …



Allianz der Wissenschaftsorganisationen

Alexander von Humboldt-Stiftung
Deutsche Forschungsgemeinschaft
Fraunhofer-Gesellschaft
Hochschulrektorenkonferenz
Leibniz-Gemeinschaft

Deutsche Akademie der Naturforscher Leopoldina – Nationale Akademie der Wissenschaften
Deutscher Akademischer Austauschdienst
Helmholtz-Gemeinschaft
Max-Planck-Gesellschaft
Wissenschaftsrat

Bedeutung der IT-Sicherheit an wissenschaftlichen Einrichtungen

Für die Arbeit an wissenschaftlichen Einrichtungen sind Dienstleistungen der Informations- und Kommunikationstechnik (IKT bzw. IT) von zunehmender Bedeutung. Damit nimmt auch die Abhängigkeit von der Funktionstüchtigkeit einer IKT stetig zu. Gleichzeitig bedarf es für hochwertiges wissenschaftliches Arbeiten in Forschung und Lehre einer angemessenen Informations- und IT-

Aktuelle neue Regelungen zur IT-Sicherheit

- Europa
  - Datenschutz-Grundverordnung (25.5.2016 / 25.5.2018)
  - NIS-Richtlinie (8.8.2016)
- Deutschland
  - IT-Sicherheitsgesetz (25.7.2015)
    - Änderte BSI-Gesetz, TMG, TKG …
    - BSI-KRITIS-Verordnung (3.5.2016)
      - Energie, Informationstechnik und Telekommunikation, Wasser, Ernährung
    - Änderung der BSI-KRITIS-Verordnung (30.6.2017)
      - Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr
  - Gesetz zur Umsetzung der NIS-Richtlinie (30.6.2017)
    - Digitale Dienste (§2 Abs. 11 BSIG)
      - Online-Marktplätze, Online-Suchmaschinen, Cloud-Computing-Dienste
  - Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (25.5.2018)

Gemeinsamkeiten

- Risikomanagement
  - § 8a Abs. 1 BSIG, Art. 25, Art. 32 DSGVO
- Meldepflichten
  - § 8b Abs. 4 BSIG, Art. 33 DSGVO
- Vorgegebene Sicherheitsstandards
  - §8, § 8a Abs. 5 BSIG, -
- Code of Conduct/branchenspezifische Standards
  - § 8a Abs. 2 BSIG, Art. 40 DSGVO
- Audit
  - § 8a Abs. 3f BSIG, Art 41f DSGVO

Artikel 25 DS-GVO

- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Privacy by Default & Privacy by Design)
  - Pseudonymisierung
  - Datenminimierung
- Dabei sind zu berücksichtigen:
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände und Zwecke der Verarbeitung
  - Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

Artikel 32: Sicherheit der Verarbeitung

- Unter Berücksichtigung des
  - Stands der Technik,
  - der Implementierungskosten und
  - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

  treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; …

Spiegelpunkte zur Verdeutlichung; nicht im Originaltext

Artikel 32: Sicherheit der Verarbeitung

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

„Belastbarkeit" im englischen „resilience"
„Fähigkeit von technischen Systemen, bei einem Teilausfall nicht vollständig zu versagen", Fehlertoleranz
NIS-Richtline übersetzt „resilience" mit „Robustheit"

Löschen

- § 20 Abs. 3 Nr. 2 BDSG — An die Stelle einer Löschung tritt eine Sperrung, soweit … eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.
- Art. 17 & 18 DSGVO — Recht auf Löschung; Recht auf Einschränkung der Verarbeitung

- IT-Systeme müssen so gestaltet werden, dass ein Löschen möglich ist.
  - Einmal-beschreibbare Medien sind fast nicht möglich.
  - Löschen in Datenbanken unter Wahrung der Konsistenz der Datenbank?

Datenübertragbarkeit

- Eine betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, …
  - Diese Daten dürfen an einen anderen Verantwortlichen übermittelt werden
  - Eine betroffene Person kann die direkte Übermittlung verlangen
  - Es gibt diverse Einschränkungen
- Es geht nicht um Daten, die von dem Verantwortlichen „erzeugt" wurden
  - Gehaltsabrechnungen
  - Prüfungsergebnisse
  - Beurteilungen
  - Untersuchungsergebnisse bei Probanden
- Die Verantwortlichen sollten dazu aufgefordert werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen.

Artikel 40 Verhaltensregeln

- (1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen.
- Ausarbeitung von Verhaltensregeln für Branchenverbände/Interessengruppen
  - Genehmigung durch Aufsichtsbehörden
- Der AKIF sieht sich als eine Interessengruppe.

Artikel 40 Verhaltensregeln

- (2) Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können Verhaltensregeln ausarbeiten …, mit denen die Anwendung dieser Verordnung beispielsweise zu dem Folgenden präzisiert wird:
  - (a) faire und transparente Verarbeitung;
  - (b) die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen;
  - (c) Erhebung personenbezogener Daten;
  - (d) Pseudonymisierung personenbezogener Daten;
  - …
  - (h) die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32;
  - …

Artikel 40: Voraussetzungen

- Abs. 4: Verfahren für die obligatorische Überwachung der Einhaltung ihrer Bestimmungen
  - Überwachung durch akkreditierte Stelle mit Fachwissen möglich (Art. 41 Abs. 1)
- Abs. 5: Verhaltensregeln müssen genehmigt werden
- Abs. 6 - 9:
  - National: Aufnahme in ein Verzeichnis und Veröffentlichung (Annahme: 1 Behörde)
  - International: Abstimmung und Vorlage bei der Kommission
    - Durchführungsakt der Kommission zur EU-weiten Geltung
    - Veröffentlichung durch die Kommission

Wissenschaft und Forschung

- Im Rahmen von „Freiheit von Forschung und Lehre" werden Wissenschaftler und Lehrende nur wenig eingeschränkt.
- IT-Sicherheitsmaßnahmen werden als Einschränkung wahrgenommen.
- Risiko:
  - Den Hochschulen und Forschungseinrichtungen werden IT-Sicherheitsmaßnahmen von außen vorgegeben.
  - Grundschutz, ISO 2700x … sind nicht an den Bedürfnissen von Forschung und Lehre ausgerichtet.
- Deshalb sollten aus der Community vorbeugend eigene Standards geschaffen werden.

Verhaltensregeln und AKIF

- Im Sprecherkreis des AKIF wurde diskutiert, ob es Sinn macht, derartige Verhaltensregeln für die Wissenschaftseinrichtungen zu erstellen
- Es wurde beschlossen eine Arbeitsgruppe „Verhaltensregeln IT-Sicherheit nach DSGVO" einzurichten
  - Leitung Dr. Ulrich Pordesch, FhG
  - Vertreter der Forschungseinrichtungen (FhG, HGF, MPG, ZKI, KfR, DFN-Verein, DFNcert
- Probleme
  - Heterogenität von Uni-Klink bis zu Studierendenverwaltung
  - Aufsichtsbehörden wollen konkrete Verarbeitung beschrieben haben
  - Keine Vertreter der Hochschulen mit einem Mandat

Probleme im Detail

- Ein Sicherheitskonzept „One size fits all" ist nicht möglich.
- Wo drückt der Schuh?
- Typische Anwendungen mit personenbezogenen Daten
  - Studierendenverwaltung (nur Hochschulen und Universitäten)
  - Humanforschung
    - Rat für Sozial- und Wirtschaftsdaten (RatSWD)
    - Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) Arbeitsgruppe Datenschutz
    - …
  - Verarbeitung von Beschäftigtendaten
  - Allgemeine Verarbeitung personenbezogener Daten
    - Protokolldaten
    - Benutzerdatenbanken
    - E-Mailservices
    - …

MAX-PLANCK-GESELLSCHAFT | 6. DFN-Konferenz Datenschutz | SEITE 17

Wie sieht eine Verhaltensregel aus?

- Konkrete Beschreibung des Prozess?
  - Studierendenverwaltung mit HIS?
  - Studierendenverwaltung?
  - Outlook Web Access 2016?
  - Web-Mail
- Welche Sicherheitsmaßnahmen?
  - Beschreibung der Einstellungen im HIS
  - „Generische" Aussagen über Verschlüsselung etc.
  - Konfigurationsbeschreibung des Outlook Web Access
  - „Generische" Aussagen über Mindestanfordungen an TLS etc.

MAX-PLANCK-GESELLSCHAFT | 6. DFN-Konferenz Datenschutz | SEITE 18

Probleme mit Verhaltensregeln

- Die Forschung ist zu heterogen!
- Es gibt nur wenige Bereiche, in denen wir weitgehend einheitliche Verarbeitungen haben.
- Verhaltensregeln sind eher gedacht für homogenere Verarbeitungen wie
  - Versichertendaten bei Krankenkassen
  - Patientendaten in Krankenhäusern
  - Adressdaten in der Werbeindustrie
- Die Aufsichtsbehörden können keine klaren Anforderungen definieren
- Deshalb ist die Arbeitsgruppe zu dem Ergebnis gekommen einen anderen Weg zu gehen:
  - Es sollen mehr die organisatorischen Aspekte eines IT-Sicherheitsmanagement-Systems (ISMS) betrachtet werden.
  - Was ist da der Bedarf einer Hochschule oder Forschungseinrichtung?

HRK ist auch aktiv

- HRK-Kommission „Digitale Infrastruktur"
- 11.10.17 Anhörung zum Thema IT-Sicherheit
- Die AKIF Arbeitsgruppe konnte dort ihre Konzepte vorstellen
- Ein Mitglied des AKIF Sprecherkreises ist Mitglied der HRK-Kommission
- Vorstellung der Fragebogen-Aktion
- Die Fragebogen-Aktion des AKIF wurde begrüßt
- Unterstützungsschreiben des Generalsekretärs der HRK

Fragebogen-Aktion

- Die AG des AKIF initiiert eine Fragebogen-Aktion, um den Bedarf der Forschungseinrichtungen und Hochschulen im Bereich ISMS zu erheben
- Fragebogen und Auswertung FhG-IAO in Stuttgart
  - Sebastian Kurowski und Heiko Roßnagel
- Die Befragung ist anonym.

Informationssicherheit in Forschungseinrichtungen und Hochschulen

	Prozesse und Regelungen des Informationssicherheitsmanagement	
I	**Meldepflicht von IT-Sicherheitsvorfällen** Die DSGVO fordert die Meldung bestimmter IT-Sicherheitsvorfälle. Diese Meldepflicht wird nur notwendig, sofern personenbezogene Daten von einem IT-Sicherheitsvorfall betroffen waren.	
I.1	Wie wichtig ist diese Meldepflicht in Ihrem Bereich?	?
I.2	Wie schätzen Sie die Herausforderungen bei der Umsetzung in Ihrem Bereich ein?	?
	Hier bitte ggf. konkrete Herausforderungen für Ihren Bereich nennen. Diese Angabe ist optional.	
I.3	Wie schätzen Sie den Bedarf für Hilfen bei der Umsetzung in Ihrem Bereich ein?	?
	Hier bitte ggf. konkreten Unterstützungsbedarf für Ihren Bereich nennen. Diese Angabe ist optional.	
II	**Risikomanagementprozesse** Gesetzliche Initiativen wie die DSGVO oder das IT-Sicherheitsgesetz sehen jeweils einen strukturierten und systematischen Ansatz zur Erfassung, Bewertung und Adressierung von Risiken vor. Solche Ansätze sind beispielsweise in Informationssicherheitsmanagement-Standards, wie ISO 27001 oder IT-Grundschutz, integriert.	
II.1	Wie wichtig ist das Risikomanagement in Ihrem Bereich?	?
II.2	Wie schätzen Sie die Herausforderungen bei der Umsetzung in Ihrem Bereich ein?	?

MAX-PLANCK-GES

Themenkomplexe

- Prozesse und Regelungen des Informationssicherheitsmanagement
  - Meldepflicht von IT-Sicherheitsvorfällen
  - Risikomanagementprozesse
  - Sicherheitskonzepte
- Maßnahmen für das Informationssicherheitsmanagement
  - Umsetzung von Datensicherheitsmaßnahmen
  - Präventive Maßnahmen
  - Datenlöschung
  - Datenportabilität
- Auditierungen, Prüfungen und Sicherheitsnachweise
  - Auditierungen und Prüfungen
  - Sicherheitsnachweise
  - Good Practices

Fragen zu den Themenkomplexen

- Wie wichtig ist dieser Aspekt in Ihrem Bereich?
- Wie wichtig sind interne Audits in Ihrem Bereich?
- Wie wichtig sind externe Audits in Ihrem Bereich?
- Wie schätzen Sie die Herausforderungen bei der Umsetzung in
- Ihrem Bereich ein?
- Wie schätzen Sie den Bedarf für Hilfen bei der Umsetzung in Ihrem
- Bereich ein?

- Antworten auf einer 5-Punkt-Likert-Skala
  - Überhaupt nicht wichtig – eher unwichtig – neutral – wichtig – sehr wichtig
  - Keine – eher geringe – neutral – eher große – sehr große Herausforderung
  - Kein – eher geringer – neutral eher – hoher – sehr hoher Bedarf

Wie geht es weiter?

- Der Fragebogen wird diese Woche verschickt.
- Die Auswertung liegt Februar/März vor.
- Am 24./25. April eine Tagung des AKIF zum Thema IT-Sicherheit und DSGVO in Berlin
  - Welcher Unterstützungsbedarf wurde identifiziert?
  - Sensibilisierung für das Thema.
  - Welche Initiativen ergeben sich daraus
  - Sind wir bis zum 25. Mai 2018 fertig? Nein. Andere auch nicht.
  - Wir sind auf dem Weg


Vielen Dank für Ihre
Aufmerksamkeit !
https://www.it-sicherheit.mpg.de