Leibniz Universität Hannover

Dienstanweisung zum Datenschutz und zur Informationssicherheit im Homeoffice und während der mobilen Arbeit

Ass. iur. Simon Graupe, LL.M. – Datenschutzbeauftragter und Leitung der Stabsstelle Datenschutz

Warum sind Datenschutz und Informationssicherheit wichtig?

Wenn die Uni plötzlich offline ist - Hackerangriff auf die Universität Gießen

Sonntag der 8.12.2019 ist für die Justus-Liebig-Universität Gießen (JLU) ein einschneidendes Datum. An diesem Tag wird der Hackerangriff auf die Universität bekannt und das **Landeskriminalamt nimmt seine Ermittlungen** auf. Wie Expert*innen vermuten, wurde die Universität Gießen mithilfe der Schadsoftware Emotet infiziert. Ein falsch geöffneter Email-Anhang und der Virus verbreitete sich schnell. Da er sich gut verbergen kann und ständig transformiert, ist es technisch sehr schwer ihn aufzuhalten.

> "Der Präsident nennt es eine "digitale Naturkatastrophe". **An der Uni Gießen geht nichts mehr: nicht die Website, nicht die Mails, nicht die Ausleihe in der Bibliothek. Niemand kann sich an den PCs einloggen, das Prüfungsamt kann keine Zeugnisse ausstellen**. Die Studierenden kommen weder an ihre Noten, noch an ihre Seminarunterlagen ran. In den Studentenwohnheimen gibt es kein WLAN mehr. Seit mehr als einer Woche sind die 28.000 Studierenden und 5.500 Mitarbeiter der Justus-Liebig-Universität offline." - Ausschnitt aus Zeit Campus vom 17.Dezember 2019

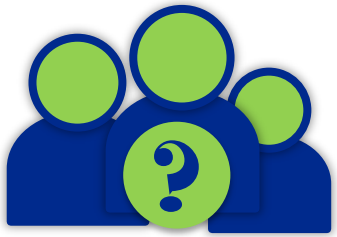
- Mobile Arbeit / Homeoffice außerhalb des geschützten Bereiches des Arbeitsplatzes innerhalb der LUH

- Datenschutz und Informationssicherheit müssen weiterhin gewährleistet sein, um missbräuchliche Nutzung / Datendiebstahl zu verhindern

Schutzbedarfsfeststellung / Risikoanalyse

Gemeinsam mit der/dem Vorgesetzten erörtern (Beispiele in der Anlage zur Dienstanweisung bieten erste Orientierungshilfe):

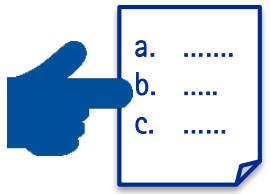
1. Welche Tätigkeiten möchte ich im Homeoffice / während mobiler Arbeit erledigen?
2. Welche Daten sind von diesen Tätigkeiten betroffen?
3. Welche Risiken können entstehen, wenn diese Daten missbräuchlich verwendet werden?

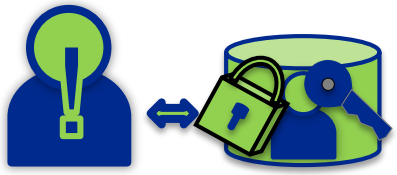


Grundlage: Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen (Schutzstufen A – E)

→ Je höher der Schutzbedarf der zu bearbeitenden Daten eingestuft wird, desto höher sind die zu ergreifenden Datensicherheitsmaßnahmen (s. Sicherheits- und Technikkonzept)

→ Schutzstufe E generell im Rahmen von mobiler Arbeit und Homeoffice verboten





Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen

Schutz-stufe	Risiko	Beispiele LUH	
A	Gering → Daten wurden von den Betroffenen frei zugänglich gemacht	• Kontaktangaben • Tätigkeitsbereiche • Publikationen	• Vorlesungsverzeichnis • Vorlesungsmaterialien / Skripte • Übungsmaterialen
B	Unsachgemäße Handhabung lässt zwar keine besondere Beeinträchtigung erwarten, die Daten wurden aber von den Betroffenen nicht frei zugänglich gemacht	• Dienstliche Daten der Beschäftigten, die die interne Organisation betreffen (Geschäftsverteilungsplan, interne E-Mail-Verteiler, Zuständigkeiten) • Tätigkeitsbezogene Angaben in Protokollen von hochschulöffentlichen Gremiensitzungen • Kontaktinformationen Dritter (Vertragspartner, Drittmittelgeber, Behörden und ähnlich verbundenen Einrichtungen)	
C	Daten, deren unsachgemäße Handhabung die Betroffenen in deren gesellschaftlichen Stellung oder in deren wirtschaftlichen Verhältnissen beeinträchtigen könnten	• Vertragsunterlagen (zu Dritten) • Rechnungen • Reise- und Lohnabrechnungen • Drittmittelverträge • Einzelne Klausuren und einzelne Prüfungsergebnisse	
D	Daten, deren unsachgemäße Handhabung die Betroffenen in deren gesellschaftlichen Stellung oder in deren wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnten	• Personalunterlagen und Personalakteninhalte • Leistungsinformationen über Studierende (z.B. Prüfungsakte, Leistungsübersicht, Abschluss) • Daten besonderer Kategorien nach Art. 9 DSGVO	
E	Unsachgemäße Handhabung könnte Gesundheit, Leben oder Freiheit der Betroffenen beeinträchtigen	• Hochsensible Strafakten, Zeugenschutzprogramme und deren Verarbeitung im Rahmen von Forschungsprojekten	

Ausgestaltung der Arbeitsplatzumgebung

Datenschutz: So viele Firmeninterna geben Mitarbeiter im Zug preis

Kaspersky Lab hat ein Datenschutz-Experiment gestartet – und einmal mitgehört und -gelesen, welche Daten man beim Zugfahren quasi nebenbei mitbekommt. Das Ergebnis sollte Führungskräften zu denken geben.

Das IT-Security-Unternehmen Kaspersky Lab hat nun fünf Tage lang einen Beobachter mit Strichliste durch Züge geschickt und ihn die Geschäftsgeheimnisse, die ihm per Auge und Ohr begegnet sind, zählen und auswerten lassen. Protokolliert wurden in fünf Tagen genau 2.245 einsehbare und mitzuhörende Informationen – Namen von Unternehmen und Kollegen, Einblicke in Präsentationen und Geschäftszahlen und Daten von Kooperationspartnern. Während des Kaspersky-Experiments konnte der beauftragte Tester 281 physische Dokumente und 1.193 Bildschirme (Laptops, Smartphones oder Tablets) mit Business-Bezug anonym einsehen. Hinzu kommen 106 mithörbare Geschäftstelefonate. Das entspricht 13 öffentlich zugänglichen

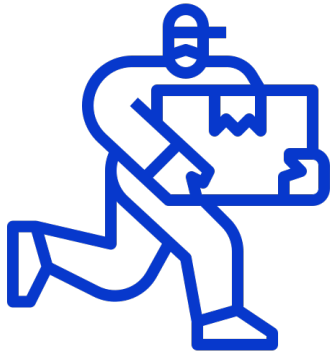
Ausgestaltung der Arbeitsplatzumgebung

Vertraulichkeit und Verfügbarkeit der Daten sollte wie im Büro sichergestellt sein, z.B.

- Der Arbeitsplatz ist so gewählt, dass unbefugte Dritte keinen Blick auf den Bildschirm und in die Papierunterlagen werfen können
- Es werden Sichtschutzfolien angeboten, wenn dies erforderlich ist
- Es gilt eine Clean-Desk-Policy, das bedeutet, dass beim Verlassen des Arbeitsplatzes alle Unterlagen sicher verschlossen werden und vor unberechtigtem Zugriff geschützt werden müssen
- Papierunterlagen müssen in Dokumentenmappen oder Schränken verschlossen werden
- Fenster werden in Erdgeschosswohnungen bei Verlassen des Arbeitsplatzes immer geschlossen
- Beim Verlassen des Arbeitsplatzes sind die Endgeräte zu sperren
- Es wird darauf geachtet, dass vertrauliche Gespräche (z.B. Telefongespräche, Videokonferenzen) nicht von unbefugten Personen oder Sprachassistenten (z.B. Alexa, Siri) mitgehört werden

Umgang mit Papierdokumenten

- Beim Umgang und insbesondere während des Transportes von Papierdokumenten besteht ein erhöhtes Verlustrisiko und damit verbunden das Risiko eines meldepflichtigen Datenschutzvorfalls
- Daher sollten nur die zwingend für die dienstliche Aufgabenerfüllung erforderlichen Dokumente außerhalb der Dienststelle transportiert werden
- Beim Transport dürfen Papierdokumente nicht unbeaufsichtigt im öffentlichen Raum bleiben und sind so zu schützen, dass Dritte keine Einsicht nehmen können
- Daten der Schutzstufe D sollen grundsätzlich nicht in Papierform im Homeoffice und während der mobilen Arbeit verarbeitet werden. Dies gilt insbesondere für Personalaktendaten oder Dokumente mit einer Vielzahl von Daten der Schutzstufe D
- Soweit möglich, soll nicht mit den Originaldokumenten, sondern mit Kopien gearbeitet werden
- Eine Entsorgung erfolgt nur über geeignete Aktenvernichter, die mindestens der Sicherheitsstufe 3 entsprechen

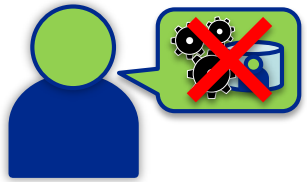


Speicherung von Dateien

- Die Speicherung von Daten hat grundsätzlich auf den üblichen Netzlaufwerken oder den von der LUH zentral zugelassenen Cloud-Speicherdiensten zu erfolgen
  - → Nur so ist gewährleistet, dass die Daten regelmäßig gesichert werden und Datenverlust vermieden wird
- Ausnahme: Wenn eine Verbindung zu den Netzlaufwerken oder Cloud-Speicherdiensten der LUH nicht möglich ist
  - Speicherung auf den Netzlaufwerken oder Cloud-Speicherdiensten der LUH ist unverzüglich nach Wiederherstellung einer Verbindung nachzuholen
  - Lokale Kopien von Daten sind anschließend zu löschen
- Aufbewahrungs- und Löschfristen gelten auch für die im Homeoffice gelagerten Daten und Dokumente

Und wenn doch mal etwas schiefgeht???

- Bei Datenschutzverstößen oder Sicherheitsvorfällen ist unverzüglich die Stabsstelle Datenschutz und/oder der/die Informationssicherheitsbeauftragte zu informieren



- Die an der LUH etablierten Prozesse gelten auch im Rahmen des Arbeitens aus dem Homeoffice und während mobiler Arbeit , vgl. insbesondere Rundschreiben 02/2019