Über die Bedeutung der Informationssicherheit

Dr. Martin Laufen[1], Dr. Rüdiger Greth[2], Isabelle Biallaß[3]

Aus der Sicht des Ressort-CISO des Ministeriums der Justiz Nordrhein-Westfalen ist These 3 ausdrücklich zu unterstützen. Nicht nur bei der Durchführung, sondern bereits bei der Planung der elektronischen Abnahme der staatlichen juristischen Prüfungen müssen die Aspekte der Informationssicherheit stets mitgedacht werden.

Informationssicherheit ist zum einen IT-Sicherheit, also der Schutz des soziotechnischen Systems aus Mensch und IT-Gerät, und zum anderen darüber hinausgehend der Schutz des Wissens und der Abläufe einer Organisation. Schutz meint dabei Schutz vor Bedrohungen, die

- die Vertraulichkeit,
- die Integrität oder
- die Verfügbarkeit

von Prozessen, Daten, Räumen oder anderen Objekten beinträchtigen können.

Diese Grundwerte müssen bei der Einführung der digitalen Prüfung beachtet werden. Vertraulichkeit bedeutet, dass sichergestellt werden muss, dass die für die digitale Prüfung relevanten Prozesse, Daten, etc. nicht unberechtigt zur Kenntnis genommen oder weitergegeben werden. Auch wenn dies wie eine Selbstverständlichkeit erscheint, sind – in Bezug auf die Papierklausur – durchaus schon Verstöße gegen diesen Grundwert bekannt geworden.

Der zweite Grundwert ist die Integrität; dies bedeutet, dass die Korrektheit der Informationen und der Funktionsweise der eingesetzten Systeme sichergestellt werden muss. Zunächst muss der Prüfling im Prüfprozess eindeutig authentifiziert und autorisiert werden. Diese Authentizität ist ein Aspekt der Integrität, die darauf zielt, dass der Ursprung der Daten festgestellt werden kann. Der Inhalt der Klausuren muss im Nachhinein unveränderbar sein. Das gleiche gilt – im Falle der elektronischen Korrektur – für die Anmerkungen der Prüfer. Bereits bei der Entwicklung der Software, mit der die digitale Prüfung abgenommen wird, sollte insbesondere dieser Punkt mitgedacht werden, z. B. in dem nicht nur der durch den Prüfling erstellte Text gespeichert wird, sondern auch dokumentiert wird, wann welche Befehle eingegeben wurden.

Zudem ist der Grundwert der Verfügbarkeit zur berücksichtigen. Autorisierte Benutzer dürfen nicht am Zugriff auf Informationen und Systeme behindert werden. Zu denken ist vor allem an den Prüfling während des für die Klausurerstellung festgesetzten Zeitraums, aber auch an die Prüfer, die Mitarbeiter des Prüfungsamts und den im Nachgang Einsicht nehmenden Prüfling.

---

[1] Ressort-CISO des Ministeriums der Justiz Nordrhein-Westfalen/Referatsleiter IT 2 (Informationssicherheit/CISO, Rechtsfragen des ERV und der E-Akte, e-Justice Projekte der EU).
[2] Leiter des Kompetenzzentrums Informationssicherheit, OLG Hamm.
[3] Referentin im Ministerium der Justiz des Landes Nordrhein-Westfalen, Referat IT 2 (Informationssicherheit, Rechtsfragen des ERV und der E-Akte, E-Justice-Projekte der EU, KI und Legal Tech).

In Kenntnis der Bedeutung der Informationssicherheit wurde im Jahr 1991 das Bundesamt für Sicherheit in der Informationstechnik (BSI) gegründet. Im Laufe der Jahre hat das BSI bestehende Standards für Informationssicherheit aggregiert und zum sogenannten „IT-Grundschutz“ ausgebildet. Mit Grundschutz ist nicht etwa „Grund“ im Sinne von „Grundversorgung“ oder „grundsätzlich“ gemeint, sondern vielmehr im Sinne von „gründlich, vollständig, ganz und gar“. Der Grundschutz richtet sich vor allem an Bundesbehörden, Landesbehörden und Wirtschaftsunternehmen und versetzt sie in die komfortable Situation, kostenlos auf einen äußerst differenzierten und spezifischen Standard zurückgreifen zu können, der von Sicherheitsexperten auf Basis aktueller Technik und Erfahrungen ausgearbeitet wurde. Die Justiz NRW hat sich, der Landesverwaltung NRW folgend, in ihrer Informationssicherheitsleitlinie[4] zu der Anwendung der IT-Grundschutz-Standards verpflichtet.

Der Grundschutz bietet zunächst eine Methodik, die sicherstellt, dass eine Organisation sich sämtlicher in ihrem Bereich relevanter Problemfelder der Informationssicherheit bewusst werden kann und mit deren Hilfe ein Sicherheitskonzept entweder für die komplette Organisation oder aber einen bestimmten Bereich, z. B. die „Digitale Prüfung“ erstellt werden kann. Mit Hilfe des Sicherheitskonzepts wird ein kontinuierlicher Verbesserungsprozess für die Organisation bzw. den bestimmten Bereich initiiert und betrieben. Das Sicherheitskonzept besteht zu Beginn im Wesentlichen aus den Stufen:

- Festlegung des Geltungsbereichs
- Identifikation der wesentlichen Prozesse und weiterer wesentlicher Objekte wie z. B. Räume und Geräte
- Festlegung des Schutzbedarfs der Prozesse und der damit verbundenen Daten

Der Grundschutz verlangt auf sämtlichen Stufen, dass die Festlegungen von der jeweiligen Organisationsleitung verantwortet werden, wobei auf den fachlichen Input der jeweils „problemnächsten“ Stellen innerhalb der Organisation zurückgegriffen werden kann und sollte. Bei dem gesamten Informationssicherheitsprozess sieht der Grundschutz eine koordinierende und kontrollierende Rolle in Gestalt eines Informationssicherheitsbeauftragten vor, der weisungsfrei agieren und unmittelbaren Zugang zur Leitungsebene haben muss.

Die IT-Grundschutz-Methodik empfiehlt drei Schutzbedarfskategorien:

- normal: Die Schadensauswirkungen sind begrenzt und überschaubar.
- hoch: Die Schadensauswirkungen können beträchtlich sein.
    - sehr hoch: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Sind die Prozesse und die Schutzbedarfe bestimmt, liefert der Grundschutz automatisch den kompletten SOLL-Zustand des Geltungsbereichs aus Sicht der Informationssicherheit, indem er im sogenannten „Grundschutzkompendium“ alle bei normalem Schutzbedarf umzusetzenden Anforderungen benennt, die für den Geltungsbereich in Frage kommen.

[4] https://lv.justiz.nrw.de/Justiz_NRW/informationstechnik/informationssicherheit/index.php.

Insofern bietet der Grundschutz neben der Methodik auch einen umfangreichen und sehr konkreten, modular aufgebauten Maßnahmenkatalog. Dieser Schritt der passgenauen Anwendung des Kompendiums auf den jeweils betrachteten Geltungsbereich nennt sich „Modellierung“. Beispielsweise ist eine Anforderung aus dem Grundschutz für den Fall, dass ein externer Dienstleister die Durchführung einer digitalen Prüfung unterstützt, vertraglich ein einheitliches Sicherheitsniveau zwischen Justiz und externem Dienstleister festzulegen:

> *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*
>
> *Alle Sicherheitsanforderungen für ein Outsourcing-Vorhaben MÜSSEN auf Basis einer Strategie zum Outsourcing festgelegt sein Beide Outsourcing-Parteien MÜSSEN sich vertraglich dazu verpflichten, den IT-Grundschutz oder ein vergleichbares Schutzniveau einzuhalten. Alle Schnittstellen zwischen dem Outsourcing-Dienstleister und -Kunden MÜSSEN identifiziert und entsprechende Sicherheitsanforderungen definiert werden. In den Sicherheitsanforderungen MUSS festgelegt sein, welche Berechtigungen wie Zutritts-, Zugangs- und Zugriffsrechte jeweils gegenseitig eingerichtet werden.*

Nach der Modellierung werden im Sicherheitskonzept der SOLL- und der IST-Zustand verglichen. Dieser Schritt wird als „Grundschutz-Check“ bezeichnet. Die sich aus dem Check ergebenden Abweichungen sowie eventuelle weitere besondere Risiken werden in einem Risikobehandlungsplan zusammengefasst. Somit hat die Organisationsleitung stets einen kompletten aktuellen Überblick über alle Risiken, die im betrachteten Geltungsbereich wichtig sind.

Im Ergebnis hilft die Informationssicherheit, speziell der IT-Grundschutz, Risiken in der Organisation oder in einem bestimmten Bereich wie z. B. der digitalen Prüfung zu erkennen, zu bewerten und zu behandeln. Zur Erhöhung der Effizienz ist es wichtig, den Informationssicherheitsbeauftragten frühzeitig bei der Planung neuer Vorhaben einzubinden (Informationssicherheit „by design“), um Informationssicherheit bei allen neuen Anwendungen und Prozessen von Anfang an mitzudenken und nicht erst nachträglich zu implementieren.