Liste von Ereignissen, die als Sicherheitsvorfälle zu bewerten sind

Lfd. Nr.	Beispiele
1.	Installation eines Schadprogramms (Viren, Würmer, Trojaner) auf IT-Systemen
2.	Hackerangriff
3.	Social Engineering Angriff (Der Begriff „Social Engineering" bezeichnet eine Vorgehensweise, bei der das Vertrauen des Einzelnen missbraucht wird. Dabei werden Mitarbeiterinnen und Mitarbeiter mit einem Trick überredet, die normalen Sicherheitsvorkehrungen zu umgehen und sensible Informationen preiszugeben.)
4.	Massenhafter Eingang von Spam-Mails (unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten, die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt enthalten)
5.	Unautorisierter Abfluss von vertraulichen/ dienstlichen Informationen z.B. - bei einem Lauschangriff (das geheime Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit technischen Mitteln) - in Beantwortung von Phishing-Mails (Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen und den entsprechenden Personen zu schaden.) - durch unerlaubte Weitergabe von Daten per Mail oder USB-Gerät - durch unsachgemäße Entsorgung von Datenträgern (Festplatten, USB-Sticks, Speicherkarten
6.	Erlasswidriges Versenden personenbezogener Nachrichten an Empfänger außerhalb der nds. Landesverwaltung; Erlass des MJ v. 23.03.2018 - 1500-103.98: (- Versand von E-Mails der Schutzstufe C und D nur mit Ende-zu-Ende-Verschlüsselung zulässig - Versand von E-Mails der Schutzstufe E gänzlich unzulässig)
7.	Weitergabe/ Diebstahl von Authentisierungsmitteln (z.B. J-Kennung, Passworte, Signaturkarten)
8.	Missbrauch von Rechten (z.B. Vortäuschen einer anderen Identität an nicht gesperrtem Arbeitsplatz)
9.	Erlasswidrige Nutzung multimedialer Internetdienste (u.a. Internet-Fernsehen, Internet-Radio)
10.	Unautorisierte Manipulation von Anwendungen, Datenbeständen und Web-Seiten
11.	Nachträgliche unbefugte Veränderung von Dateien (Urteil, Beschluss, Protokoll etc.)
12.	Direkte Veränderung von Daten in der Datenbank unter Umgehung der Fachanwendung ohne dokumentierte Genehmigung der betroffenen Behörde
13.	Anschluss von • gefundenen oder nicht dienstlichen USB-Sticks an Justizhardware • privaten Druckern • nicht dienstlicher / privater Hardware, mit Ausnahme von: o kabelgebundenen Mäusen und Tastaturen o nicht-internetfähigen Monitoren o sonstigem nicht-internetfähigen Zubehör (z. B. WebCams, Mikrofonen, Headsets)

Lfd. Nr.	Beispiele
	• nicht vom ZIB unterstützter Hardware oder • Hardware mit veraltetem Betriebssystem (Windows NT, Windows XP) an das Justiznetz
14.	Nutzung von • externen Festplatten oder • unerlaubter Software (nicht durch den ZIB gemanagt/ keine Einzelfreigabe durch MJ) im Justiznetz
15.	Verlust oder Diebstahl von Dateien (auf Servern, PCs, Notebooks oder USB-Sticks)
16.	Verlust, Zerstörung oder Diebstahl von Hardware (PCs, Notebooks, Tablets, Smartphones, Festplatten, USB-Sticks)
17.	Einbruch in eine Behörde
18.	Versuchtes oder erfolgreiches unbefugtes Eindringen in das Rechenzentrum oder in den Systembetriebsraum einer Behörde
19.	Speicherung in unautorisierten Clouddiensten
20.	Speichern von illegalen Daten auf Justizhardware (Musik/Filme) außer zum Zwecke der Beweismittelsichtung bzw. -verwendung
21.	Erhebliche Störung/ Fehlfunktion/ Ausfall von • IT-Systemen und Fachanwendungen (z.B. EUREKA, HWS, web.StA) • zentralen Diensten / Services (z.B. Active Directory, E-Mail-Dienst, Internet- oder Intranetzugang) • Standard-Software • Netzwerkhardware des ZIB und IT.N • Infrastrukturdiensten (z.B. der Klimaanlage, Telekommunikation, USV, Netzersatz-anlagen)
22.	Eine Behörde oder eine größere behördenübergreifende Gruppe von mindestens 400 Anwenderinnen und Anwendern kann unvorhersehbar nicht arbeiten
23.	Ausfall von Hardware durch Stromausfall, Wasserschäden, Feuereinwirkung, Baustaub, Überspannungsschäden/Gewitter