LWVHessen

Informationssicherheits-bericht 2025

FuB 102.5 IT-Verwaltungsangelegen-heiten und Informationssicherheit

Inhalt

Vorwort

Liebe Leserinnen und Leser,

„Das einzig sichere System müsste ausgeschaltet, in einem versiegelten und von Stahlbeton ummantelten Raum und von bewaffneten Schutztruppen umstellt sein."

– Gene Spafford

Mit diesem aus dem Jahr 1989 stammenden Zitat sprach der renommierte US-amerikanische Informationssicherheitsexperte Gene Spafford ein Thema an, dessen Relevanz inzwischen um ein Vielfaches zugenommen hat: Mit der weltweiten Digitalisierung von Daten stellt sich heute mehr denn je die Frage, ob es Informationssicherheit* überhaupt gibt und was man tun kann, um sich vor Sicherheitsvorfällen zu schützen.

Die Antwort auf den ersten Teil der Frage lautet: Nein, es gibt keine absolute oder garantierte Sicherheit. Auch noch so gute technische Systeme können keinen 100-prozentigen Schutz vor Cyberangriffen* garantieren. Im Gegenteil – stetig spitzt sich die Bedrohungslage weiter zu und die Komplexität steigt, was sich im Detail im jährlichen Bericht des Bundesamtes für Informationstechnik (BSI) zur Lage der IT-Sicherheit* in Deutschland ablesen lässt. Allein angesichts der hierin ausgewiesenen Anzahl an neuen Schadprogramm*-Varianten von täglich mehr als 300.000 (!) lautet die entscheidende Frage nicht ob, sondern vielmehr wann man Opfer eines Cyberangriffs* wird. (siehe Kapitel 1)

Cyberangriffe*: Die unvermeidbare Realität

Und hiervon gibt es immer mehr in allen Bereichen der Gesellschaft: Wirtschaft, Politik, Behörden und Privatpersonen. Besorgniserregend ist vor allem, dass Angreifer gezielt Schwachstellen in IT-Systemen nutzen, um kritische Infrastrukturen zu stören.

Im Jahr 2025 führten Angriffe auf einen Leistungserbringer und eine Rechtsanwalts- und Steuerberatungskanzlei zu einem unautorisierten Datenabfluss. Davon betroffen waren auch Daten des LWV. Dazu hat der Ransomware*-Angriff einen Großteil der Infrastruktur betroffen, so dass ein normales Arbeiten in beiden Betrieben über mehrere Wochen hinweg nicht mehr möglich war.

Diese Vorfälle führen uns vor Augen, welche katastrophalen Folgen damit verbunden sein können und wie nah die Gefahr auch an den LWV herankommen kann.

Wie wäre der LWV mit einem Ausfall seiner Fachverfahren und einem dadurch verursachten Krisenmodus umgegangen?

Sinnvolle Vorbereitungen: Schlüssel zum Erfolg

Allerdings – und damit kommen wir zum Positiven – kann man sehr wohl eine Menge tun, um sich zu schützen. Eine zunehmend entscheidende Rolle spielt dabei – neben umfassenden technischen und organisatorischen Schutzmaßnahmen – die Vorbereitung auf den Ernstfall, um bspw. für den Ausfall der Fachverfahren gewappnet zu sein. Besonders öffentliche Verwaltungen wie der LWV, die auf ein reibungsloses Funktionieren ihrer IT-Systeme angewiesen sind, sollten der kritischen Bedrohungslage mit einem durchdachten Business Continuity Management (BCM)* begegnen. Ziel eines BCM* ist es, die betriebliche Einsatzfähigkeit eines Unternehmens in Krisensituationen aufrechtzuerhalten bzw. nach einem Angriff schnellstmöglich wieder in geordnete Strukturen zu gelangen. (siehe Kapitel 3)

Ein weiterer wichtiger Schlüssel zum Erfolg ist der Mensch. Daher haben wir im Juni 2025 eine Sensibilisierung zur Stärkung und Erweiterung des Bewusstseins für

Informationssicherheit* und Datenschutz* begonnen. (Siehe Kapitel 4)

Liebe Leserinnen und Leser, lassen Sie sich von diesem Bericht dazu inspirieren, die Informationssicherheit* im Alltag zu leben und mitzugestalten. Der Weg zu optimalem Schutz führt nur über Sie!

Kassel im Januar 2026

Peter Pfeffer

Informationssicherheitsbeauftragter

1. Allgemeine Lage der Informationssicherheit* in Deutschland

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland informiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) jährlich über die Bedrohungslage im Cyberraum. Im Bericht für das Jahr 2025 kommt die Cybersicherheitsbehörde des Bundes zur Einschätzung: Für die Lage der IT-Sicherheit in Deutschland besteht im Berichtszeitraum weiterhin keine Entwarnung. Die IT-Sicherheitslage bleibt weiterhin auf einem angespannten Niveau.

Nachfolgend sind Informationen aus dem Lagebericht 2025 des BSI wiedergegeben, um die Informationssicherheitslage in Deutschland wiederzugeben.

Die Informationssicherheitslage in Deutschland bleibt auf angespanntem Niveau. Durch die fortschreitende Digitalisierung wachsen Angriffsflächen, die zu schlecht geschützt werden. Im Kontext geopolitischer Konflikte nehmen APT*-Aktivitäten zu.

Die weiterhin angespannte Lage ist auch auf zu viele immer noch zu schlecht geschützte Angriffsflächen zurückzuführen. Viele Behörden, Unternehmen und andere Organisationen machten es Angreifern nach wie vor zu leicht, sodass diese mit vergleichsweise geringem Aufwand und einfachen Mitteln weiterhin großen Schaden anrichten konnten. Denn Angreifer gingen mehr und mehr den Weg des geringsten Widerstandes und suchten sich jene Ziele aus, die am leichtesten angreifbar waren, das heißt deren Angriffsflächen das niedrigste Schutzniveau aufwiesen. Das betraf insbesondere kleine und mittlere Unternehmen sowie Institutionen des politischen und vorpolitischen Raums, deren Web-Angriffsflächen nicht ausreichend geschützt waren. Nach dem Kosten-Nutzen-Kalkül cyberkrimineller Angreifer gibt es keine uninteressanten Ziele mehr, bei denen vermeintlich „nichts zu holen“ wäre. Jede aus dem Internet erreichbare Institution oder Person ist prinzipiell bedroht, jede und jeder ist ein interessantes Ziel. Im aktuellen Berichtszeitraum führte dies unter anderem dazu, dass Schwachstellen zunehmend ausgenutzt (Exploitation*) und mehr Daten exfiltriert und veröffentlicht wurden (Datenleaks*). Eine gesamtgesellschaftliche Steigerung der Präventionsfähigkeiten durch ein wirksames Angriffsflächenmanagement aufseiten der Verteidiger ist daher das Gebot der Stunde.

Die Lage im Einzelnen:

1. Bedrohungslage: Stabilisierung auf hohem Niveau

Im Cybercrime-Bereich führten internationale Strafverfolgungsmaßnahmen zu einer Stabilisierung der Bedrohungslage. Zwei vormals sehr aktive Angreifergruppen haben ihre Aktivitäten nahezu vollständig eingestellt. Demgegenüber war im Kontext geopolitischer Konflikte eine Zunahme an APT*-Aktivitäten in den betroffenen Regionen zu verzeichnen. Zudem wurden im aktuellen Berichtszeitraum neue Angriffsinfrastrukturen bekannt. Insbesondere zwei neue, große IoT*-Botnetze* fielen durch Schadsoftware auf, die bereits im Produktionsprozess auf Geräte gelangt war. Da die Geräte bereits vorinfiziert in den Handel kamen und auch nicht nachträglich bereinigt werden konnten, gab es für Nutzende keine wirksamen Gegenmaßnahmen. Betroffen waren rund 40.000 IoT*-Geräte.

2. Angriffsfläche: Web-Angriffsflächen werden bedeutender

Die Angriffsflächen in Deutschland wachsen im Zuge der Digitalisierung. Präventive Maßnahmen müssen Schritt halten. Unter den aus dem Internet erreichbaren .de-Domains boten im aktuellen Berichtszeitraum noch rund 61 Prozent ausschließlich das

alte, weniger sichere IPv4-Protokoll* an. Darüber hinaus waren bei 47 Prozent der erreichbaren IP-Adressen hinter .de-Domains sensible Informationen öffentlich aus dem Internet einsehbar, darunter Geoinformationen oder sogar Informationen über potenzielle Schwachstellen. Auch digitale Kommunikationswege wie E-Mail-Adressen, Social-Media-Accounts, Messenger-Accounts und SMS-fähige Telefonnummern bieten weiterhin große, schwer zu schützende Angriffsflächen. Darüber hinaus können Schwachstellen in jeglicher Form von IT-Produkten auftreten. Im aktuellen Berichtszeitraum wurden durchschnittlich täglich 119 neue Schwachstellen bekannt, ein Wachstum von rund 24 Prozent gegenüber dem vergangenen Berichtszeitraum, das nur teilweise auf eine veränderte Meldepraxis zurückzuführen war. Schwachstellen in Perimetersystemen* waren – wie schon in den vergangenen Jahren – ein wichtiges Einfallstor für Cyberangriffe.

3. Gefährdungslage: Mehr Schwachstellen-Exploits*, mehr Datenleaks*

Die Gefährdungslage war im aktuellen Berichtszeitraum weiterhin angespannt. Die Zahl der angezeigten Ransomware*-Angriffe blieb nach Erkenntnissen des Bundeskriminalamts mit 950 weitgehend unverändert. Cyberkriminelle setzten dabei erfolgreiche Angriffsstrategien der letzten Jahre fort. So wurden nicht nur immer mehr kleine und mittlere Unternehmen angegriffen (80 Prozent der angezeigten Angriffe). Die Angriffe führten in den meisten Fällen auch zu Datenleaks* (bzw. deren Androhung), gegen die es aufseiten der Geschädigten keine Bewältigungsstrategien gibt. Backups bleiben essenziell gegen Ransomware*, helfen aber nicht gegen Datenleaks*. Zudem erpressen Angreifer auch immer häufiger mit Daten, die sie aus unzureichend gesicherten Datenbanken oder aus schwachstellenbehafteten Systemen im Internet exfiltrieren. Auch hier helfen nur wirksame Präventivmaßnahmen im Rahmen eines strukturierten Angriffsflächenmanagements. Hinsichtlich der Angriffsvektoren zeigte sich im Berichtszeitraum daher folgerichtig, dass die Ausnutzung von Schwachstellen in Web-Angriffsflächen mittels Exploitation* weiter an Bedeutung gewann. Angriffe per E-Mail gingen demgegenüber spürbar zurück. Hintergrund dürfte unter anderem die weitere Verlagerung von digitaler Kommunikation auf andere Kanäle wie etwa Social Media oder Messenger sein, die Angreifer ebenfalls seit Jahren zunehmend für die Verteilung von Malware*- oder Phishing*-Mails nutzen. Das Angriffsflächenmanagement vielfältiger digitaler Kommunikationswege stellt eine besondere Herausforderung dar.

4. Schadwirkungen: Mehr Datenleaks*, weniger Lösegelder

Die größten Schadwirkungen erzielten Angreifer im aktuellen Berichtszeitraum weiterhin mit Ransomware* in Verbindung mit Datenleaks*. Bedeutsamer wurden aber auch reine Datenleaks*. Kerngeschäft der Cyberakteure ist hier immer noch die Erpressung. Die Erbeutung von Zugangsdaten, die sich im Darknet gut weiterverkaufen lassen, spielt jedoch eine immer größere Rolle. So stieg nicht nur die Zahl der durch Datenabfluss unmittelbar geschädigten Unternehmen und anderen Institutionen. Da häufig Kundendaten auf unzureichend gesicherten Webservern betroffen waren, waren auch mehr Geschäftskunden sowie Verbraucherinnen und Verbraucher als Einzelpersonen mittelbar betroffen. Die Summe der insgesamt gezahlten Lösegelder ist zurückgegangen. Dies resultiert daraus, dass Cyberangreifer mehr und mehr auch mittlere, kleine und Kleinstunternehmen mit schwach geschützten Angriffsflächen angreifen, und zwar selbst dann, wenn diese je Fall weniger Lösegeld erwarten lassen.

5. Resilienz: Digitale Sorglosigkeit verbreitet sich

Resilienzmaßnahmen stehen zwar zur Verfügung, allerdings ist im zweiten Jahr in Folge ihr Bekanntheitsgrad unter den Verbraucherinnen und Verbrauchern gesunken und sie werden weniger angewandt. Das betraf insbesondere die Verwendung und das Management von sicheren Passwörtern. Um dem Trend zur Verwendung unsicherer Passwörter entgegenzuwirken, bieten sich Passkeys an, das heißt kryptografische Schlüsselpaare, die zum Beispiel unkompliziert mittels Fingerabdruck freigegeben werden können.

Kritische Infrastrukturen: Langsame, stetige Verbesserung

Die Resilienz der Kritischen Infrastrukturen wächst langsam, aber stetig. Immer mehr Betreiber erfüllen inzwischen die Mindestanforderungen (Reifegrad 3), es zeigen sich jedoch noch deutliche Abstufungen zwischen den Präventions-, Verteidigungs- und Bewältigungsfähigkeiten. Während rund 80 Prozent der Betreiber bereits ein Informationssicherheits-Management-System (ISMS)* mit einem Reifegrad von mindestens 3 führten, lag der Anteil bei Business-Continuity-Management*-Systemen mit knapp zwei Dritteln deutlich darunter. Bei Systemen zur Angriffserkennung besteht hingegen noch deutlicher Nachholbedarf (48 %).

Kleine und mittlere Unternehmen: Alle sind gefährdet – viele, ohne es zu wissen

Flächendeckende Resilienz der kleinen und mittleren Unternehmen (KMU) in Deutschland bleibt eine große Herausforderung. Vielen mangelt es nicht nur an Wissen und Fähigkeiten zur Informationssicherheit, sondern bereits an der grundlegenden Einsicht, dass sie sehr wohl ein lohnendes Ziel für Cyberangriffe darstellen. Hintergrund dürfte eine grundlegende Fehleinschätzung der Bedrohungs- und Gefährdungslage sein: Für cyberkriminelle Angreifer sind weder Umsatz noch Branche ausschlaggebende Kriterien der Zielauswahl, sondern der Aufwand für den Angriff muss in einem günstigen Verhältnis zum erwarteten Nutzen stehen. Und dieser Aufwand steigt, je besser potenzielle Ziele geschützt sind. Angreifer suchen daher gezielt nach den verwundbarsten Angriffsflächen, denn gerade auch Angriffe auf kleine und Kleinstunternehmen lohnen sich, wenn der Aufwand vergleichsweise gering ist. Ziel für Unternehmen jeder Größe muss es also sein, sich durch möglichst gut geschützte Angriffsflächen unattraktiv für Cyberkriminelle zu machen.

Institutionen des vorpolitischen und politischen Raums: „Kronjuwelen“ der Demokratie in Deutschland müssen cyberresilient werden

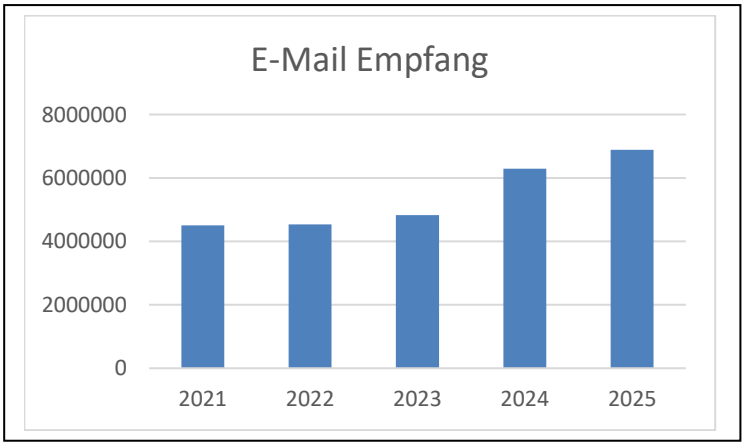
Wie die KMU haben sich auch politische und politiknahe Stiftungen, Vereine, Verbände sowie politische Parteien noch gar nicht als attraktives Ziel für potenzielle Cyberangriffe erkannt. Dabei bieten sie unter Umständen nicht nur direkte Zugänge zu politischen Entscheidungsträgern, sondern auch sensible Informationen über nicht öffentliche und halböffentliche politische Debatten sowie über die politischen Willensbildungsprozesse in Deutschland. Im Rahmen fremdstaatlicher Destabilisierungsstrategien gegen demokratische Institutionen in Deutschland sind derartige Informationen von entscheidendem Wert. Sie sind oftmals wichtige Voraussetzungen für Informationsoperationen, die beispielsweise politische Stimmungen beeinflussen sollen oder die ganz grundsätzlich auf die Destabilisierung der Demokratie in Deutschland zielen. Vorgaben für die Cyberresilienz der Institutionen, die die demokratische politische Willensbildung in Deutschland tragen, werden bislang noch nicht gesetzlich geregelt. Die wehrhafte Demokratie sollte dies dringend nachholen.

2. Aktuelle Bewertung der Informationssicherheit* im LWV

Bezogen auf den Berichtszeitraum 2025 ist die Lage der Informationssicherheit* im LWV trotz der angespannten Gesamtlage insgesamt als positiv zu bewerten.

Diese positive Bilanz ist im Wesentlichen auf den bestehenden Informationssicherheitsprozess, beschrieben in der Leitlinie Informationssicherheit* (Ziffer 5.3 im Organisationshandbuch) und seine konsequente Umsetzung durch die Mitarbeitenden zurückzuführen, insbesondere auch im Hinblick auf deren Achtsamkeit.
Die Realisierung erfolgt als laufender Prozess im Rahmen des im LWV etablierten Informationssicherheits-Management-Systems (ISMS)*, welches nach dem Grundschutzkompendium, dem anerkannten Standard für Informationssicherheit* des BSI, aufgebaut ist und durch die Mindeststandards für die Informationssicherheit des LWV Hessen als verbindliche Vorgabe gilt.

Es gab keine nennenswerten IT-Sicherheitsvorfälle im LWV. Bezeichnend für das Jahr 2025 ist aber der Anstieg der Bedrohungslage. Im Gegensatz zu den vergangenen Jahren hat der LWV deutlich mehr E-Mails empfangen, sogar gegenüber dem Jahr 2024 hat sich der Wert noch erhöht. So gab es einen Anstieg um 600 Tausend auf 6,88 Millionen. Ein Großteil davon, in Höhe von 5,13 Millionen, waren E-Mails, die potenzielle Bedrohungen enthielten.



Weiterhin ist zu beobachten, dass die Anzahl gezielter Phishing*-Mails im Berichtszeitraum abermals stark zugenommen hat. Die Phishing*-Mails haben dabei sehr an Qualität gewonnen, was eine Identifizierung durch die Mitarbeitenden des LWV zunehmend erschwert.
Dieser Trend wird durch den Einsatz von KI und Einbindung von Deep Fakes* voraussichtlich auch immer weiter zunehmen.

Zum Aufbau eines präventiven Schutzes vor Cyberangriffen* setzt der LWV eine Reihe von Systemen ein:

- Der LWV betreibt eine mehrstufige und mit unterschiedlichen Virenschutzprogrammen ausgestatte Infrastruktur, die sowohl die PCs, die Server, die Dateien als auch die Verbindungen zum Internet schützt.
- Zentrale E-Mail-Gateways* überprüfen alle eingehenden E-Mails und sorgen dafür, dass die meisten davon erst gar nicht ins LWV-Netz gelangen, weil es sich eindeutig um unerwünschte Werbung oder Schad-Mails handelt.
- Für die sichere E-Mail-Kommunikation werden Verschlüsselungs-Gateways* genutzt. Über diesen Weg besteht die Möglichkeit, sicher und datenschutzkonform personenbezogene Daten mit externen Kontakten auszutauschen.
- Sämtliche Internetinhalte, die von LWV-Mitarbeitenden aus dem Internet angefordert werden, laufen über einen sog. Proxy. Diese Art Filter verfügt über einen Antivirusschutz und überprüft die Web-Inhalte mittels Sandboxing*.

3. Notwendigkeit eines Notfallkonzepts

Die Entwicklung eines strukturierten Notfallkonzepts ist ein wesentlicher Bestandteil einer ganzheitlichen Risikovorsorge und dient dem Schutz der betrieblichen Kontinuität. Ziel ist es, auf potenzielle Ausfälle – sei es durch technische Störungen, Cyberangriffe*, Naturereignisse oder menschliche Fehler – vorbereitet zu sein und im Ernstfall handlungsfähig zu bleiben.

Ein erster und entscheidender Schritt ist die Identifikation der kritischsten Geschäftsprozesse und damit verbundenen Anwendungen und Systeme, deren Ausfall den Geschäftsbetrieb unmittelbar gefährden würde. In einer gemeinsamen Arbeitsgruppe mit den verantwortlichen Organisationseinheiten sind die kritischsten Geschäftsprozesse bestimmt und in einer sogenannten Minimalbetriebs-Matrix aufgenommen worden.

Auf dieser Grundlage können geeignete Maßnahmen definiert werden, um im Notfall den Betrieb dieser Kernfunktionen – ggf. in reduzierter Form – aufrechtzuerhalten oder schnellstmöglich wiederherzustellen. Dazu werden in einem zweiten Schritt die IT-Systeme und DV-Verfahren identifiziert, die für einen Weiterbetrieb oder die Wiederaufnahme der kritischsten Geschäftsprozesse dringend benötigt werden.

Ein solches Notfallkonzept reduziert wirtschaftliche Schäden, minimiert Ausfallzeiten und erhöht das Vertrauen von Leistungsberechtigten, Partnern und Aufsichtsbehörden in die Resilienz des LWV. Zudem schafft es Klarheit über Rollen, Verantwortlichkeiten und Kommunikationswege im Krisenfall. Des Weiteren sollen die folgenden Ziele erreicht werden:

- Verbesserung der Entscheidungsfindung in Krisenzeiten
- Verbesserte Bewältigung der wachsenden Bedrohungslandschaft
- Förderung der Präventionskultur
- Kontinuierliche Verbesserung
- Regulative Compliance
- Schutz der Reputation

Der Aufbau eines funktionierenden Notfallkonzepts stellt daher einen zentralen Beitrag zur langfristigen Sicherung der Funktionsfähigkeit des LWV Hessen dar.

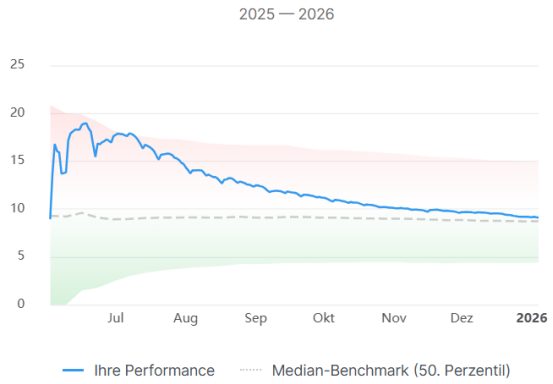
4. Die wichtige Rolle der Mitarbeitenden

Daten und vertrauliche Informationen sind wertvoll. Informationsschutz und Informationssicherheit* erfordern die Aufmerksamkeit der Behördenleitung. Eine wachsende Zahl von technischen Komponenten, Tools und Lösungen können physikalische Barrieren errichten und Zugangswege versperren oder reglementieren. Doch über 80 Prozent aller bekannten Sicherheitsvorfälle werden laut eines Studienberichts des Bitkom* von Beschäftigten – oft unbewusst – verursacht, weil sie technische Systeme umgehen und/oder Sicherheitsregeln nicht beachten. So werden die meisten Schäden durch Unwissenheit, Bequemlichkeit und Gewohnheit verursacht. Deshalb müssen sowohl die Technik wie auch „der Faktor Mensch“ beim Informationsschutz und der Informationssicherheit* berücksichtigt werden. Nur wenn die Bereiche Mensch und Technik ausreichend Beachtung finden, sichere und funktionierende Prozesse existieren, die Anwenderinnen und Anwender den Nutzen der Maßnahmen verstehen und ihr Verhalten anpassen, ist ein Maximum an Informationssicherheit* gewährleistet.
Damit Beschäftigte Daten des LWV Hessen aktiv schützen, müssen sie die Gefahren kennen und ein Bewusstsein für den richtigen Umgang entwickeln. Regeln und Prozesse sollen ihnen dabei helfen und sie unterstützen. Im Idealfall entwickeln sie einen geschulten Blick für die Risiken im eigenen Handlungsbereich und werden proaktiv tätig, um Schaden vom LWV Hessen abzuwenden. Sie achten auf die Einhaltung der Regeln im LWV Hessen und weisen auch neue Kolleginnen und Kollegen, Praktikantinnen und Praktikanten sowie Auszubildende ein.

Damit dies gelingt, werden alle Mitarbeiterinnen und Mitarbeiter der Haupt- und Regionalverwaltungen, der Gedenkstätte in Hadamar, der Stiftungsforsten in Haina und der Verwaltungen der Förderschulen, die sich in Trägerschaft des LWV Hessen befinden, (ca. 1500 Personen) seit dem 01.06.2025 im Rahmen eines E-Learnings sowie einer Phishing*-Simulation in Fragen der Informationssicherheit* und des Datenschutzes* geschult und sensibilisiert.

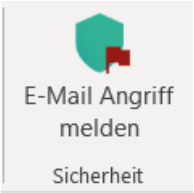
Phishing*-Simulation

Im ersten Jahr des Sensibilisierungszeitraums werden 20 Phishing*-E-Mails versendet, die zum Anklicken eines potentiell gefährlichen Links oder Anhangs motivieren sollen. Die Links in den Phishing*-E-Mails verweisen jedoch ausschließlich auf Aufklärungs-/Lernseiten. Es besteht keine Gefahr für die Mitarbeiterinnen und Mitarbeiter, die Daten des LWV Hessen oder die Endgeräte. Darüber hinaus werden keine Daten über das individuelle Klickverhalten von Personen gesammelt.



Die Klickrate beschreibt den Anteil der versendeten E-Mails, bei denen auf ein Phishing*-Element (z. B. Bild, Link, Dateianhang) geklickt wurde. Sie ist im Jahresverlauf deutlich gesunken und liegt zum Jahresende bei 9,1 %. Damit nähert sie sich dem Medianwert jener anderen öffentlichen Einrichtungen, die ebenfalls das Awareness-Programm unseres Anbieters nutzen (8,72 %). Dieser Trend zeigt, dass sich das sicherheitsbewusste Verhalten spürbar verbessert.

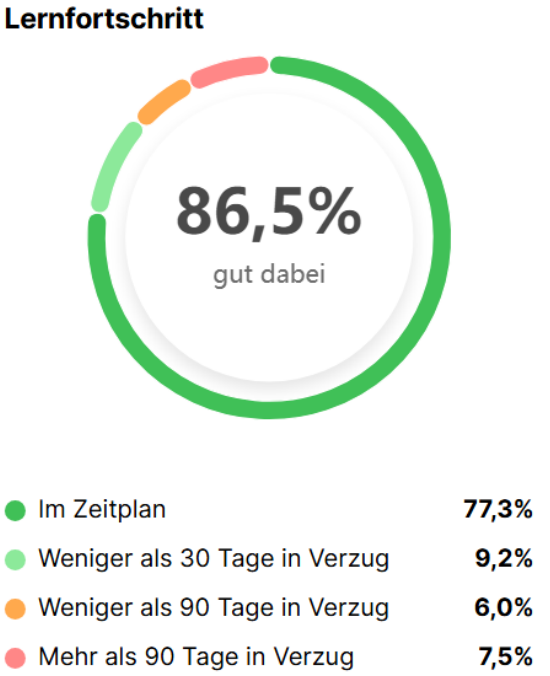
Phishing*-Melde-Button



Die Einführung des Phishing*-Melde-Buttons ist eine wichtige Maßnahme, um die Sicherheit der digitalen Kommunikation zu erhöhen. Phishing*-Angriffe werden immer raffinierter und können sensible Daten, wie persönliche Informationen oder Zugangsdaten, gefährden. Durch einen einfachen und in Outlook integrierten Melde-Button können Mitarbeitende verdächtige E-Mails schnell und unkompliziert melden, so dass die IT-Abteilung sofort reagieren und entsprechende Schutzmaßnahmen ergreifen kann. Das stärkt die Sicherheitskultur innerhalb der Verwaltung, reduziert das Risiko von Datenverlusten und schützt sowohl die Daten unserer Mitarbeitenden als auch die Daten der uns anvertrauten Menschen. Insgesamt trägt der Melde-Button dazu bei, das Bewusstsein für Informationssicherheit* zu erhöhen und die Verwaltung widerstandsfähiger gegen Cyberangriffe zu machen.
Besonders erfreulich ist die eindeutig erkennbare positive Tendenz der Melderate. Sie ist seit Programmstart auf inzwischen 26,71 % gestiegen – und dies in einem durchgehend kontinuierlichen Verlauf. Dieser stetige Zuwachs zeigt sehr klar, dass immer mehr Mitarbeitende verdächtige Inhalte nicht nur erkennen, sondern auch aktiv melden. Damit entwickelt sich eine zunehmend lebendige und wirksame Sicherheitskultur innerhalb des LWV Hessen.

E-Learning

Ergänzend zu der Phishing*-Simulation wurde für alle Mitarbeitenden ein Zugriff auf ein spezielles und individuell gestaltetes E-Learning-Angebot zum Thema Informationssicherheit* und Datenschutz* eingerichtet. Die Module sind sehr kompakt gehalten und beinhalten jeweils ein spannendes Quiz am Ende.
Nach erfolgreicher Registrierung wird ein kurzer Fragebogen durchlaufen. Daraus resultiert der persönliche und individuell gestaltete Lernpfad, den es über die nächsten Monate zu bearbeiten gilt.
Die Absolvierung der entsprechend gekennzeichneten Module ist verpflichtend. Die Teilnahme sowie der Fortschritt werden mithilfe von regelmäßigen Reports nachgehalten. Der Aufwand für das E-Learning beschränkt sich für die Mitarbeitenden im Durchschnitt auf ca. 5 Minuten pro Woche.



Der Fortschritt zum Jahresende ist äußerst positiv zu bewerten: 86,5 % der Mitarbeitenden gelten als „gut dabei“, absolvieren das Training also innerhalb des vorgegebenen Zeitplans oder nur mit einer leichten Verzögerung.

5. Spezielle Sicherheitsmaßnahmen 2025

Im Bereich Informationssicherheit bedeutet Stillstand Rückschritt. Es gilt daher, den bestehenden Schutz durch ein Bündel spezieller technischer, organisatorischer und personeller Maßnahmen kontinuierlich weiter zu verstärken. Im Folgenden möchten wir Ihnen einige Beispiele für den Berichtszeitraum 2025 aufzeigen.

Weiterführung des ISMS*

Die konsequente Fortführung des Informationssicherheits-Management-Systems (ISMS)* ist entscheidend für den Schutz von Informationen, Systemen und Betriebsprozessen. Sie stärkt Transparenz, Rechts- und Sicherheitskonformität sowie die Resilienz des LWV gegenüber Bedrohungen und betrieblichen Störungen. Die ISMS*-Fortführung ist damit eine Investition in Kontinuität und Vertrauenswürdigkeit.
Eine klare Unterstützung durch die oberste Verwaltungsebene ist unverzichtbar, um Risiken proaktiv zu managen, Compliance sicherzustellen und Vertrauen bei Kunden, Partnern und Mitarbeitenden zu stärken.

IT-Risikomanagement

Im Rahmen der Faxnutzung im LWV ist eine IT-Risikoanalyse durchgeführt worden. Die unverschlüsselte Übermittlung von personenbezogenen Daten mit einem besonderen Schutzbedarf (insb. Sozialdaten) per Fax bietet keine ausreichende Sicherheit und stellt damit einen Verstoß gegen die Anforderungen der Datenschutzgrundverordnung und der Mindeststandards für Informationssicherheit des LWV Hessen dar.
Bis zur endgültigen Ablösung der Faxnutzung ist das Risiko durch die Behördenleitung akzeptiert worden.

IT-Notfallhandbuch

Das IT-Notfallhandbuch ist aktualisiert und im Organisationshandbuch unter der Ziffer „4.1.6 EDV-Notfallmaßnahmen“ veröffentlicht worden. Dieses Dokument umfasst alle Aspekte der Notfallbewältigung und beinhaltet konkrete Handlungsanweisungen. Es soll die Verantwortlichen des LWV Hessen in die Lage versetzen, einen geordneten Notbetrieb zu erreichen. Alle Regelungen, die den Notbetrieb selbst betreffen, sind in den weiterführenden Dokumenten zur Fortführung der IT-Verfahren geregelt.
Die Begriffe Störung, Notfall, Krise und Katastrophe sind definiert. Dazu wird namentlich benannt, wer eine/ein IT-Notfallverantwortliche/r ist. Die Liste der IT-Notfallverantwortlichen ist im ISMS* eingestellt und wird dort fortlaufend aktuell gehalten.

IT-Sicherheitskonzept

Für das IT-Verfahren A21 Leistungs- und Vergütungsdatenbank wurde ein IT-Sicherheitskonzept erstellt. Hier kamen neu entwickelte Vorlagen zum Einsatz, die sowohl die IT-Sicherheitsanforderungen laut den Mindeststandards beinhalten als auch gleichzeitig als umfassende Dokumentation für das IT-Verfahren dienen.
Damit konnte der Aufwand der Dokumentation auf das Wesentliche reduziert werden.
IT-Sicherheitskonzepte für andere IT-Verfahren wurden begonnen.

IT-Sicherheitsrichtlinie

Die Sicherheitsrichtlinie Sicherer IT-Betrieb und IT-Administration ist um die Kapitel „Cloud Nutzung“ sowie „Beschaffung und Vertragsgestaltung“ erweitert worden.
Die Implementierung klarer Cloud-Richtlinien und vertraglicher Rahmenbedingungen erhöht Transparenz, Kontrolle, Informations- und Rechtssicherheit. Dies stärkt die operative Effizienz der Administratoren und reduziert Risiken in Beschaffung, Betrieb und Incident-Management*.

6. Ausblick

Folgt man den Prognosen von Informationssicherheitsfachleuten, wird sich die Bedrohungslage weiter verschärfen, sowohl was die Anzahl als auch die Vielschichtigkeit der Angriffe anbelangt. Um dem zu begegnen, sind auch für die nähere Zukunft weitere Maßnahmen geplant.

Für das Jahr 2026 rückt die Informationssicherheit erneut die folgenden Themen in den Mittelpunkt.

- Die Fortführung des ISMS* – Sicherstellung der fortlaufenden Anpassung an neue Bedrohungen, Technologien und regulatorische Vorgaben.
- Überprüfung und Anpassung der Mindeststandards für Informationssicherheit des LWV Hessen
- Fortführung der umfassenden Mitarbeiterschulungen zu Informationssicherheit und Datenschutz
- Unterstützung bei IT-Sicherheitskonzepten und Risikoanalysen
- Weiterführung der Ausarbeitungen der Arbeitsgruppe Notfallkonzept, um im Ernstfall besser vorbereitet zu sein

Dies sind zentrale Eckpfeiler, um Rechts- und Sicherheitsanforderungen zu erfüllen, Betriebsunterbrechungen zu minimieren und Vertrauen bei internen wie externen Stakeholdern zu stärken.

Die Sicherheit unserer Informationen ist unverzichtbar für den Schutz von Werten, Reputation und Geschäftsfähigkeit. Die regelmäßige Fortführung des ISMS*, gezielte Schulungen und eine klare Unterstützung bei Sicherheitskonzepten und Risikoanalysen sind essenzielle Investitionen in einen sicheren, zuverlässigen und zukunftsfähigen LWV.

Die Unterstützung der obersten Verwaltungsebene ist hierfür unverzichtbar.

Glossar

APT (Advanced Persistent Threat)

Ein APT ist ein meist von Nationalstaaten unterstützter Cyberangriff, der auf Spionage oder Sabotage abzielt. APT-Angriffe bleiben oft über längere Zeiträume hinweg unerkannt im System, was ihnen den Namen „persistent“ verleiht.

Bitkom

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) vertritt mehr als 2300 Unternehmen der digitalen Wirtschaft; darunter 1000 Mittelständler, 300 Start-ups und nahezu alle Global Player.

Botnetz

Ein Botnetz ist ein Netzwerk von kompromittierten und fernsteuerbaren Geräten, wie PCs, Smartphones oder IoT-Geräten, die von Cyberkriminellen für schädliche Zwecke missbraucht werden. Die Besitzer bemerken oft nicht, dass ihre Geräte Teil eines Botnetzes sind. Häufige Ausprägungen sind das Versenden von Spam, die Durchführung von DDoS*-Angriffen (Denial of Service*-Angriff), Datendiebstahl oder das Ausführen von Angriffen auf andere Systeme.

BSI Grundschutzkompendium

Das IT-Grundschutz-Kompendium stellt die Grundlage des IT-Grundschutzes dar und bildet zusammen mit den BSI-Standards die Basis für das Thema Informationssicherheit*.

Business Continuity Management

Ein Business Continuity Management (BCM) bezeichnet einen Prozess, mit dem sich ein Unternehmen, bspw. für den Fall eines Cyberangriffs, auf die Identifikation von Risiken und die Aufrechterhaltung bzw. die Wiederherstellung des Geschäftsbetriebs vorbereitet.

Cyberangriff

Ein Cyberangriff ist ein Versuch, Computer außer Betrieb zu setzen, Daten zu stehlen oder ein angegriffenes Computersystem für weitere Angriffe zu nutzen.

Darknet

Als Darknet wird ein nicht über herkömmliche Wege erreichbarer Bereich im Internet bezeichnet, der eine anonyme Kommunikation innerhalb bestimmter Gruppen ermöglicht. Das Darknet wird häufig von Kriminellen für den Vertrieb illegaler Ware oder für die Planung von Straftaten genutzt.

Datenleak

Ein Datenleak ist die unautorisierte Offenlegung vertraulicher oder persönlicher Daten, die unbeabsichtigt durch menschliche Fehler, technische Schwachstellen oder aber gezielt durch böswillige Angriffe (Cyberangriffe*) geschehen kann. Die Informationen können dabei an Dritte gelangen, von denen sie zu Missbrauch, beispielsweise für Identitätsdiebstahl, genutzt werden.

Datenschutz

Während die Informationssicherheit* den Schutz sämtlicher Informationen zum Ziel hat, stellt der Datenschutz sicher, dass niemand die Kontrolle über die seine Person betreffenden Daten verliert. Umfasst sind alle Daten, die sich auf eine identifizierbare Person beziehen, wie bspw. Name, Geburtsdatum oder auch E-Mail-Adressen. Diese Daten dürfen von Dritten wie Unternehmen oder Behörden nur im Einklang mit den Prinzipien der Datenschutz-Grundverordnung (DSGVO) verarbeitet werden.

DDoS-Angriff

Bei einem DDoS-Angriff (Distributed Denial of Service) – eine bestimmte Art von

Cyberangriff – überfordert ein Angreifer eine Website, einen Server oder eine Netzwerkressource mit schädlichem Traffic.

Deep Fakes

Werden mithilfe einer Künstlichen Intelligenz Audiodateien oder Videos derart manipuliert, dass der fälschliche Eindruck entsteht, eine Person hätte eine bestimmte Aussage getätigt oder sich in einer bestimmten Art und Weise verhalten, spricht man von sog. Deep Fakes. Sie werden meistens dazu verwendet, um in der Öffentlichkeit stehenden Personen Schaden zuzufügen. Deep Fakes können mittlerweile mit sehr einfachen technischen Mitteln erstellt werden und stellen dadurch eine wachsende Gefahr da.

Exploit/Exploitation

Ein Exploit (englisch „to exploit“: ausnutzen) ist ein kleines Schadprogramm (Malware*) bzw. eine Befehlsfolge, die Sicherheitslücken und Fehlfunktionen von Hilfs- oder Anwendungsprogrammen ausnutzt, um sich programmtechnisch Möglichkeiten zur Manipulation von PC-Aktivitäten (Administratorenrechte usw.) zu verschaffen oder Internetserver lahm zu legen.

Gateway

Mithilfe eines Gateways können verschiedene, an sich inkompatible Systeme, miteinander kommunizieren. Dafür fungiert das Gateway als Schnittstelle und wandelt bspw. Daten eines Netzwerks in ein Format um, das von einem anderen Netzwerk verarbeitet werden kann.

Internet of Things (IoT)

Internet of Things (IoT) bezeichnet ein Netzwerk aus physischen Geräten, die mit Sensoren und Software ausgestattet sind, um über das Internet miteinander zu kommunizieren und Daten auszutauschen. Diese vernetzten „smarten“ Geräte reichen von einfachen Haushaltsgeräten wie Thermostaten und Smartwatches bis hin zu komplexen industriellen Maschinen und können für Automatisierung, Effizienzsteigerung und Datenerfassung genutzt werden.

IPv4-Protokoll

IPv4 steht für Internet Protocol Version 4 und ist der vierte und bisher am weitesten verbreitete Standard für die Adressierung und den Datentransport in Netzwerken und im Internet. Es weist jedem Gerät eine eindeutige Nummer zu (z. B. 192.168.1.1), die aus vier durch Punkte getrennten Zahlenblöcken besteht. Da die verfügbaren IPv4-Adressen aufgrund des begrenzten Adressraums von etwa 4,3 Milliarden fast aufgebraucht sind, wird zunehmend auf den Nachfolger IPv6 umgestellt.

IT-Sicherheit / Informationssicherheit

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.
Nicht zu verwechseln ist die IT-Sicherheit mit der Informationssicherheit, welche den Schutz von Informationen zum Ziel hat. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwenderinnen und Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein.

Incident-Management

Incident-Management ist ein Prozess, der darauf abzielt, Störungen oder ungeplante Unterbrechungen von IT-Diensten schnell

zu erkennen, zu analysieren und zu beheben, um den normalen Geschäftsbetrieb so rasch wie möglich wiederherzustellen. Das Hauptziel ist, die Auswirkungen von Vorfällen zu minimieren, Ausfallzeiten zu reduzieren und die Servicequalität aufrechtzuerhalten.

Informationssicherheits-Management-System (ISMS)

Ein Informationssicherheits-Management-System umfasst die Gesamtheit aller Methoden, Verfahren und Regeln innerhalb einer Organisation, die die Informationssicherheit* erhöhen.

Near Field Communication (NFC)-Tags

NFC (ermöglicht den drahtlosen Austausch von Informationen mit mobilen Endgeräten, wie zum Beispiel einem Smartphone, welches mit NFC ausgerüstet ist. Viele aktuelle Geräte (Android, Blackberry und Windows) sind bereits mit einer entsprechenden Schnittstelle ausgestattet.

Perimetersystem

Eine "Perimeter System Firewall" ist ein Sicherheitssystem, das eine Firewall nutzt, um die äußere Grenze (das Perimeter) eines privaten Netzwerks (z. B. eines Unternehmensnetzes) vor dem öffentlichen Internet zu schützen. Dieses System überwacht und filtert den gesamten ein- und ausgehenden Datenverkehr, um schädliche oder unerwünschte Daten abzuwehren und unbefugten Zugriff zu verhindern.

Phishing

Das Wort setzt sich aus „Password“ und „Fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“. Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, an Zugangsdaten für einen Dienst oder eine Webseite zu gelangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten u. U. selbst unwissentlich in unberechtigte Hände. Bekannte Beispiele sind Phishing-Angriffe gegen Bankkunden, die in einer E-Mail aufgefordert werden, ihre Zugangsdaten auf der Webseite der Bank einzugeben und validieren zu lassen.
Mit dem gleichen Verfahren werden aber auch Nutzer von E-Commerce-Anwendungen (z. B. Online-Shops oder Online-Dienstleister) angegriffen. Angreifer setzen zunehmend Schadprogramme* statt klassischem Phishing als Mittel zum Identitätsdiebstahl ein. Andere Varianten des Phishings setzen auf gefälschte Near Field Communication (NFC)-Tags* oder Barcodes, die vom Opfer eingelesen werden und auf eine Phishing-Seite weiterleiten.

Ransomware

Als Ransomware werden Schadprogramme* bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch: „ransom“) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

Sandboxing

Sandboxing ist eine Cybersicherheitsmethode, bei der Code oder Dateien in einer sicheren, isolierten Umgebung (der „Sandbox“) ausgeführt werden, um ihre Sicherheit zu testen, ohne das eigentliche System zu gefährden. Diese isolierte Umgebung imitiert das echte Betriebssystem, erlaubt aber keinen Zugriff auf sensible Ressourcen wie Dateisystem oder Netzwerk, sodass schädliches Verhalten wie Viren-Aktionen analysiert werden kann, ohne Schaden anzurichten, bevor die Software freigegeben wird.

Schadprogramm / Schadsoftware / Malware

Die Begriffe Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus „Malicious software“ und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.