BUNDESNOTARKAMMER
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

Handreichung IT-Sicherheit für Notarinnen und Notare sowie deren Beschäftigte

Bundesnotarkammer

Stand: April 2022

Inhaltsverzeichnis

Ein typischer Montagmorgen…

Dr. Monika Müller, erfolgreiche Notarin in einem achtköpfigen Notarbüro, fuhr ihren Arbeitsplatzrechner hoch. Alles schien wie immer: Der Kaffee war frisch, das Postfach gefüllt und die erste Beurkundung stand unmittelbar bevor. Nach diesem ersten Termin galt es, die anstehende Woche sowie die aktuellen Akten und Entwürfe mit den Beschäftigten zu besprechen.

Doch mit den digital abgespeicherten Vorgängen stimmte etwas nicht. Die Dateien hatten plötzlich ganz andere Namen. Sie öffnete das erste Dokument: Anstelle einer letztwilligen Verfügung waren lediglich kryptische Zeichen zu sehen. Sofort öffnete sie weitere Dateien: Das Gleiche. Bei den Beschäftigten ebenso. Das ganze Büro konnte offenbar keine Entwürfe oder sonstige Dateien mehr öffnen.

Beunruhigt rief Notarin Müller ihren Systembetreuer an und nach einer kurzen Analyse stand fest: Das Notarbüro wurde Opfer einer Ransomware-Attacke. Das Schlimmste dabei: Die Dateien wurden nicht nur verschlüsselt, sondern auch gestohlen. Die Hacker forderten ein Lösegeld von 1,3 Bitcoin (ca. 50.000 €), andernfalls würden sämtliche erbeuteten Informationen Datei für Datei im Internet veröffentlicht werden. Gibt sie dieser Forderung nach, wendet sie im besten Fall zwar die Veröffentlichung ab, jedoch werden sich die Angreifer ihre Zahlungsbereitschaft notieren, sodass nicht unwahrscheinlich ist, dass Frau Müller künftig erneut ins Visier gerät. Sie war schockiert. Wie konnte das nur passieren?

Allmählich erkannte der Systembetreuer, wie es zu der Katastrophe kommen konnte. Ein Mitarbeiter hatte in der vergangenen Woche einen vermeintlichen Entwurf per Mail erhalten. Doch die angehängte Word-Datei war leider mehr als nur ein harmloser Kaufvertrag. Sie war mit Schadsoftware infiziert, die sich nach dem Öffnen auf dem System unbemerkt von selbst installierte. Mangels aktuellen Antiviren-Programms hatte der Trojaner leichtes Spiel. Er gab den Angreifern die Möglichkeit, auf das Netzwerk zuzugreifen und sich darin zu bewegen. Diese freuten sich über die einfache Struktur des Netzwerks, auszutricksende Sicherheitsmechanismen existierten nicht. Das Passwort „notar1“ war ebenfalls kein nennenswertes Hindernis, sodass sich die Angreifer ungestört nach wertvollen Daten umsehen konnten. Die „Beute“ hatte der Trojaner zunächst ins Internet übertragen und anschließend verschlüsselt. Zu allem Überfluss hatte er damit erst am Wochenende begonnen, um das Entdeckungsrisiko möglichst zu minimieren.

Der Angriff ist nun eine Woche her. Eine Woche, in der niemand arbeiten konnte. Denn vor dem Einspielen der Backups musste unbedingt sichergestellt sein, dass die Systeme absolut frei von der Schadsoftware sind. Und das bedeutete letztendlich die komplette Neuinstallation vieler Komponenten.

Ein erfolgreicher Coup für die Hacker, eine Katastrophe für Notarin Müller, ihre Beschäftigten, die betroffenen Bürgerinnen und Bürger sowie die vorsorgende Rechtspflege – insgesamt jedoch ein Vorfall, der vermeidbar gewesen wäre.

Einleitung

Die IT hat sich in den letzten Jahrzehnten zu einem wesentlichen Bestandteil unserer Gesellschaft – sowohl im Privat- als auch im Berufsleben – entwickelt. Informationen werden zunehmend elektronisch verarbeitet. Das Elektronische Urkundenarchiv oder das auf die europäische Digitalisierungsrichtlinie zurückgehende notarielle Online-Verfahren im Gesellschaftsrecht verdeutlichen diese Tendenz auch im Notariat. Durch die immer umfangreichere Verknüpfung wesentlicher Abläufe mit unserer IT-Umgebung entstehen allerdings nicht nur neue Möglichkeiten, sondern auch neue Gefahren. IT-Systeme und elektronisch gespeicherte Informationen sind stets davon bedroht, kompromittiert, manipuliert oder beschädigt zu werden; die eingesetzten Methoden werden immer professioneller. Hierdurch werden Arbeitsabläufe gestört und Wirtschaftsteilnehmer finanziell geschädigt. Der Gesamtschaden umfasst in aller Regel mehr als ein Lösegeld: Hinzu treten teils beträchtliche Kosten zur Bereinigung und Wiederherstellung der Systeme, ein etwaiger Betriebsausfall sowie mitunter auch Schadensersatzforderungen der Betroffenen. Daneben – und aufgrund der Verschwiegenheitspflicht deutlich gravierender – entsteht ein immaterieller Schaden, für Betroffene wie Amtsträger.

Die Informationssicherheit zielt auf den adäquaten Schutz von Informationen und IT-Systemen, insbesondere in Bezug auf die Schutzziele „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“. So soll Gefahren für Informationen und Daten – unabhängig vom Personenbezug – weitestgehend vorgebeugt werden. Vor dem Hintergrund der notariellen Verschwiegenheitspflicht ist dieses Ziel prioritär. Zur Erreichung eines angemessenen Sicherheitsniveaus muss dabei zunächst der Ist-Zustand der Informationssicherheit im eigenen Notarbüro festgestellt werden. Nur so können (technische und organisatorische) Maßnahmen zur Erreichung des gewünschten Soll-Zustandes abgeleitet werden. Grundlegend gilt es, ein Bewusstsein für den Stellenwert der Informationssicherheit zu schaffen, da Bedrohungen maßgeblich durch unzureichende Ausstattung und unsachgemäße Handhabung begünstigt werden und sich viele Angriffe – trotz sich ändernder Technologien – durch einfache und mitunter auch bekannte Grundregeln vermeiden lassen. Die nachfolgenden Empfehlungen bieten eine **Hilfestellung** bei der Erreichung dieses Soll-Zustandes.

- **Teil I** bezweckt eine sachgemäße Handhabung und weist **Notarinnen und Notare sowie deren Beschäftigte** auf bekannte Sicherheitsrisiken und deren Folgen hin.
- **Teil II** erläutert organisatorische und technische Details **vornehmlich für Dienstleister und technisch Interessierte.**
- **Beiden Teilen** ist eine **Checkliste als Kurzüberblick** vorangestellt.

Das Eingangsbeispiel klingt überspitzt, beschreibt jedoch eine tatsächlich erfolgte und immer häufiger auftretende Ransomware-Attacke. In den Fokus geraten dabei längst nicht nur große Unternehmen, Behörden oder Krankenhäuser, sondern auch Notarbüros und zwar – aufgrund der vertraulichen Daten, der sensiblen Verschwiegenheitspflicht sowie der Bedeutung der vorsorgenden Rechtspflege – **unabhängig von deren Größe**. Die Annahme „für mich interessiert sich sowieso kein Hacker“ stellt einen – leider noch immer verbreiteten – Irrtum dar:

Jede Person und jede Organisation ist ein potenzielles Opfer, mit dem sich Geld verdienen lässt.

Kurzüberblick Teil I

Teil I: Allgemeine Sicherheitshinweise	
1. Awareness	
Werden Beschäftigte vor der Erstnutzung der IT-Systeme zum Thema IT-Sicherheit geschult?	
Wird das Problembewusstsein in regelmäßigen Zeitabständen aufgefrischt?	
Wird das Problembewusstsein durch praxisorientierte Übungen vertieft?	
2. Social Engineering	
Sind Social-Engineering-Techniken (insb. die verschiedenen Varianten des Phishings sowie der sog. „CEO-Fraud“) und deren Erkennungsmerkmale bekannt?	
Werden Anfragen auf ihre Plausibilität und Dateien erforderlichenfalls durch den Systembetreuer überprüft?	
Sind die (besonders) gefährlichen Dateiformate bekannt?	
Werden die Dateiendungen nach den Einstellungen des Betriebssystems angezeigt?	
Werden praxisorientierte, vertiefende Übungen wie Phishing-Tests durchgeführt?	
Beachtet jede Internetseite des Notarbüros das Gebot der Informationssparsamkeit?	
Sind Notar und Beschäftigte für die Relevanz der Informationssparsamkeit sensibilisiert?	
Ist das Rundschreiben 04/2021 der Bundesnotarkammer zur Cloud-Nutzung bekannt?	
3. Sichere Konten	
Werden personalisierte Benutzerkonten und Passwörter verwendet?	
Werden die nachfolgenden Hinweise zur Passwortsicherheit bei eigenen Passwörtern und denen der Beschäftigten beachtet? • Mindestkomplexität • Nicht in einem Wörterbuch zu finden • Verschiedene Passwörter für verschiedene Dienste • Anforderungen an die physische Aufbewahrung • Verbot der Weitergabe • Änderung voreingestellter Passwörter sowie bei Verdacht der Kompromittierung	
Wurden die Passwörter besonders gefährdeter Dienste überprüft?	
Werden Passwörter grundsätzlich nicht automatisch im Browser gespeichert?	
Werden Passwortmanager eingesetzt?	
Wird bei den genutzten Diensten eine Mehr-Faktor-Authentisierung verwendet?	
4. Aktualisierungen von Systemen (vgl. hierzu auch Teil II)	
Werden Systeme (insb. Betriebssystem und Software) aktuell gehalten und sind Notar und Beschäftigte für die Relevanz der Aktualisierung sensibilisiert?	
5. Sichere Nutzung des Internets	
Sind die Erkennungsmerkmale unseriöser Internetseiten bekannt?	
Wird auf eine sichere Verbindung zur aufgerufenen Webseite geachtet?	
Wird beim Download von Dateien auf deren Herkunft geachtet?	

6. Sensible Bereiche und Geräte	
Werden (organisationskritische) Geräte durch organisatorische Maßnahmen geschützt?	
Sind Arbeitsplatzrechner durch organisatorische Maßnahmen blickgeschützt?	
Ist an jedem Arbeitsplatzrechner die automatische Bildschirmsperre aktiviert?	
Werden Bildschirme bei Verlassen des Arbeitsplatzes manuell gesperrt?	
7. Mobile Speichermedien	
Wird die Nutzung dritter mobiler Speichermedien untersagt oder vorab überprüft?	
Werden einheitliche mobile Speichermedien verwendet?	
Wird das Speichern auf mobilen Speichermedien auf ein Mindestmaß reduziert?	
8. Besonderheiten bei der Mobilarbeit	
Werden die VPN-Zugangsdaten und Passwörter besonders geschützt?	
Werden Bildschirme bei Verlassen des Arbeitsplatzes manuell gesperrt?	
Werden Sichtschutzfolien verwendet?	
Werden Daten auf Netzlaufwerken abgelegt?	
Werden Mobiltelefone ausreichend geschützt? • Aktivierte Bildschirmsperre • App-Download nur aus seriösen Quellen • Vermeidung von Jailbreaking und Rooting • Verbindung nur mit bekannten oder seriösen Geräten	

Anwendungshinweis

Es handelt sich bei der Handreichung insgesamt um **rechtlich unverbindliche Empfehlungen** der Bundesnotarkammer. Das Farbschema des Kurzüberblicks dient dabei lediglich der **Priorisierung** dieser Empfehlungen, wobei eine Einstufung in die Priorisierungsgrade „hoch“, „mittel“ und „niedrig“ erfolgt.

Diese Priorisierung wird im Fließtext zur leichteren Abgrenzung der einzelnen Empfehlungen sowie aus Gründen der Einheitlichkeit aufgegriffen und durch die Wortwahl „muss“, „darf nur/nicht“, „soll“ und „kann“, „empfohlen“ dargestellt.

Die **Unverbindlichkeit** der Handreichung bleibt durch die Priorisierung **unberührt**.

TEIL I – Allgemeine Sicherheitshinweise

1. Bewusstsein schaffen

Awareness

Der Begriff „Awareness“ bedeutet im Kontext der Informationssicherheit, dass bestimmte Personen sich der Grundlagen der Informationssicherheit, der Bedrohungslage sowie etwaiger (abstrakter wie konkreter) Gefahren bewusst sind und ihr Verhalten hiernach ausrichten.

Das Problembewusstsein in Hinblick auf die IT-Sicherheit trägt maßgeblich zur Erhöhung des Sicherheitsniveaus einer Organisation wie etwa eines Notarbüros bei, da es das Verhalten der Nutzer beeinflusst. Dieses Verhalten hat wiederum einen essentiellen Einfluss darauf, ob und wie Systeme geschützt werden und – in der Folge – ob die Sicherheit im angemessenen Umfang gewährleistet wird. Der „Umweg“ über den Nutzer ist in allen Fällen der einfachste Weg für Angreifer.

Systeme sind nur dann umfassend geschützt, wenn passende Maßnahmen implementiert, akzeptiert und (auf Dauer) umgesetzt werden. Notarinnen und Notare müssen entsprechende Vorkehrungen treffen und diese zur Erhöhung und Beibehaltung des Sicherheitsniveaus den Beschäftigten vorleben, damit die Schutzmaßnahmen nicht aufgrund von Unwissenheit oder Bequemlichkeit umgangen werden.

Technische Maßnahmen können ihre Wirkung verlieren, wenn sich Notarinnen und Notare sowie deren Beschäftigte nicht angemessen verhalten. Eine zentrale Speicherung samt ausgearbeitetem Wiederherstellungskonzept ist nutzlos, wenn Urkundsentwürfe dennoch lokal abgespeichert werden und ihre Verfügbarkeit somit bei Verlust oder Beschädigung des Gerätes nicht gewährleistet ist. Gleiches gilt für physische Maßnahmen: Eine Schließanlage kann keine Eindringlinge abhalten, wenn aus Bequemlichkeit Türen offengelassen werden und Systeme so gegenüber Gefahren, wie z. B. Diebstahl oder Beschädigung, ungeschützt sind. Organisatorische Maßnahmen (z. B. Verhaltensrichtlinien) sind dabei am stärksten vom Verhalten der Adressaten abhängig, da sie – im Gegensatz zu physischen und technischen Maßnahmen – einer aktiven Umsetzung bedürfen. So verfehlen komplexe Passwörter ihren Zweck, wenn diese auf ein unter der Tastatur liegendes Blatt Papier notiert werden.

Zur Förderung des zuvor beschriebenen Bewusstseins müssen die Beschäftigten durch auf das Notariat zugeschnittene Schulungen sensibilisiert werden. Die IT-Infrastruktur sollte nicht ohne Einweisungsmaßnahmen und Kenntnis der grundlegenden Verhaltensregeln verwendet werden, sodass insbesondere neue Beschäftigte zu unterweisen sind. Im Übrigen sollten die Schulungen in regelmäßigen Abständen erfolgen und deren Inhalt sowie die jeweiligen Teilnehmenden dokumentiert werden. Praxisorientiere Übungen (vgl. Teil I Abschnitt 2.1) helfen das Wissen zu vertiefen.

2. Social Engineering

Social Engineering

Social Engineering (sog. „Soziale Manipulation“) beschreibt Methoden, die auf die Beeinflussung des Verhaltens der Nutzer abzielen: Angreifer versuchen die Nutzer zur Durchführung einer bestimmten Handlung (z. B. Anklicken eines Links) oder zur Preisgabe relevanter Informationen (z. B. Anmeldedaten) zu verleiten, meist durch eine Beeinflussung auf psychologischer Ebene. Häufige in diesem Zusammenhang an die Nutzer kommunizierte Anreize sind Vertrauen, Angst, Neugier oder auch Druck, um den Anweisungen des Angreifers Nachdruck zu verleihen. So wird in Phishingnachrichten meist eine hohe Eilbedürftigkeit zur Erzeugung von Druck vorgetäuscht.

Social Engineering erfolgt in verschiedenen Formen und über verschiedene Kommunikationskanäle (E-Mail, SMS, Telefon, persönliche Ansprache oder auch Fax). Hervorzuheben sind insbesondere Telefongespräche. *Dies verdeutlichen jüngst erfolgte Anrufe von vermeintlichen Beschäftigten der Bundesnotarkammer, die sich aufgrund angeblich erforderlicher Aktualisierungen für das Programm XNotar mittels Fernwartung Zugriff auf die Arbeitsplatzrechner verschaffen wollten*. Die Beschäftigten sollten daher (telefonische) Anfragen in Ruhe auf ihre Plausibilität überprüfen, bevor sie handeln. Es sollte immer kritisch hinterfragt werden, welche Informationen und Daten an den Anfragenden weitergegeben werden dürfen. Im Zweifel ist mit der Notarin oder dem Notar Rücksprache zu halten.

2.1 Phishing

Die mittlerweile bekannteste Form von Social Engineering ist das sog. „Phishing“ mithilfe von E-Mails. Eine in Wahrheit gefälschte E-Mail soll hierbei den Eindruck der Echtheit erwirken, um den Nutzer zum Anklicken von Links oder zur Ausführung einer angehängten, mit Schadsoftware infizierten Datei zu bewegen. Derartige E-Mails werden regelmäßig massenweise an zufällige Empfänger versendet in der Hoffnung, dass irgendjemand die gewünschte Handlung vornimmt.

Schadsoftware

Schadsoftware ist ein Oberbegriff für sämtliche Software, die (aus Sicht des Nutzers) unerwünschte Aktionen ausführt. Es lassen sich verschiedene Arten von Schadsoftware in Bezug auf *Verhaltensweise*, *Einsatzzweck* und *Schaden* unterscheiden. Die bekanntesten Arten sind Viren, Würmer und Trojaner. Einige weitere bekannte Arten sind Zeitbomben, die erst nach einer bestimmten Wartezeit aktiv werden, sowie Ransomware, die den Zugriff auf Daten oder Rechner verhindert und das Opfer einer Lösegeldforderung aussetzt. Gelegentlich setzen die Angreifer das Opfer durch eine schrittweise Veröffentlichung der erbeuteten vertraulichen Daten bis zur Lösegeldzahlung zusätzlich unter Druck.

Zu den besonders gefährlichen Datei-Formaten zählen dabei .exe, .cmd, .scr, .bat (ausführbare Formate). Daneben kann sich der Schadcode aber auch über Microsoft-Office-Dateien (z. B. durch Makros) einschleichen. In den Einstellungen von Betriebssystem und Software sollten die Dateiendungen stets vollständig angezeigt werden und entsprechende Dateien vor dem Öffnen von einem in IT-Fragen kompetenten Beschäftigten oder dem Systembetreuer überprüft werden. Je nach den technischen Möglichkeiten kann sich die Deaktivierung von Office-Makros anbieten, sofern dies mit der eingesetzten Notarsoftware vereinbar ist.-Ein per se ungefährliches Dateiformat existiert (leider) nicht.

Gezielter gehen Angreifer beim sog. „Spear Phishing“ vor. Hier werden nutzerbezogene Informationen und Präferenzen integriert. Die Tatsache, dass immer mehr (persönliche) Informationen und Bilder auf sozialen Netzwerken geteilt werden, erleichtert dabei das Vorgehen der Angreifer. Eine Phishing-Mail könnte hier einen vermeintlichen Gutschein für das Lieblingsrestaurant enthalten, der sich tatsächlich als eine kompromittierte Datei entpuppt. Der erhöhte Individualisierungsgrad steigert die Erfolgschancen. Ebenso könnten die erforderlichen Informationen zum Zurücksetzen des Passwortes herausgefiltert werden. Herkömmliche Sicherheitsfragen lassen sich so meist ohne Probleme beantworten. Da das Zurücksetzen des Passwortes bei den notariellen Fachanwendungen durch den Notar bzw. die Notarin aus dem Notarnetz erfolgen muss, besteht diese Gefahr insbesondere bei sonstigen Anwendungen wie Cloud-Diensten. Entsprechend dem Grundsatz der Informationssparsamkeit dürfen daher nur relevante Informationen im Internet geteilt werden, wobei dies zunächst die Internetseite des Notarbüros betrifft. Daneben sollten aber auch Beschäftigte sensibilisiert werden, was sie über ihren Arbeitsplatz auf ihren persönlichen Konten in den sozialen Medien preisgeben.

Technische Maßnahmen wie eine geeignete Erkennungssoftware können unerwünschte und schadhafte Nachrichten herausfiltern und so die von Phishing-Angriffen ausgehende Bedrohung minimieren. Nichtsdestotrotz stehen bei derartigen Angriffen maßgeblich die Nutzer im Fokus. Die Abwägung, ob auf einen Link geklickt wird oder Zugangsdaten preisgegeben werden, können diese nur selbst vornehmen. Daher sollte das Notarbüro hierzu aufklären, die Beschäftigten schulen und sie insbesondere auf die Erkennungsmerkmale von Phishing E-Mails hinweisen.

Hinweis

Zu den Merkmalen von Phishing-E-Mails zählen insbesondere

- falsche Absenderadressen (aufgrund minimaler Abweichungen meist nur schwer erkennbar)
- allgemein gehaltene Anreden (die Mail soll gerade „Jeden“ ansprechen)
- grammatikalisch inkorrekte Formulierungen sowie Rechtschreibfehler.

Daneben bieten sich maßgeblich im Bereich E-Mail-Sicherheit praxisorientierte Übungen an, beispielsweise durch selbsterstellte Phishing-Kampagnen, deren Ergebnisse statistisch erfasst werden können. Beschäftigte erhalten hier echt aussehende Phishing-Nachrichten aus einem Trainingssystem. Klicken

diese einen entsprechenden Link an, erhalten sie einen Hinweis, dass sie auf eine Phishing-Nachricht hereingefallen sind und müssen daraufhin eine zuvor ausgewählte Kurzschulung durchlaufen. Durch derartige Simulationen lernen die Beschäftigten auch fortschrittliche Angriffe zu erkennen.

Im Zweifel sollte kompetente Hilfe eingeholt werden. Erster Ansprechpartner ist auch insoweit der Systembetreuer des eigenen Notarbüros.

2.2 CEO-Fraud

Neben den klassischen Phishing-Angriffen existieren weitere Bedrohungen, die unter dem Namen „CEO-Fraud“, „Business-E-Mail-Compromise“ oder auch „Forged-Mail" bekannt sind. Hier sendet der Angreifer vermeintlich unter dem Namen eines Vorgesetzen – Notar oder Sozius – eine Nachricht an Beschäftigte und weist eine Zahlung an. Das Hauptmerkmal dieser E-Mails ist der direkte Bezug zur Tätigkeit der Organisation (z. B. die Anweisung einer Auszahlung von einem Anderkonto). Durch sog. „E-Mail Spoofing“ können bekannte Absenderadressen gezielt vorgetäuscht werden. Für die empfangende Partei sieht es daher so aus, als sei die verwendete E-Mail-Adresse korrekt und die Nachricht echt. Die Wahrscheinlichkeit, dass Beschäftigte den Weisungen des (vermeintlichen) Vorgesetzten vertrauensvoll Folge leisten, ist daher hoch.

Für klassische Sicherheitssysteme ist diese Art von Angriffen kaum zu erkennen, da hierbei weder Schadsoftware noch gefälschte Links, sondern nur das Vertrauen der Beschäftigten ausgenutzt wird. Echten Schutz bietet hier die „Awareness“ sowie ein kritisches Mitdenken und Hinterfragen der Beschäftigten. Aufgrund des in aller Regel „kurzen Dienstweges“ in Notarbüros bietet sich vor der Ausführung auch hier eine Rücksprache mit der Notarin oder dem Notar oder das „Vier-Augen-Prinzip“ an.

3. Sichere Konten

3.1 Personalisierte Benutzerkonten

Bei Verwendung desselben Benutzerkontos durch mehrere Beschäftigte wäre nicht nachvollziehbar, welcher Beschäftigte welche Änderungen vorgenommen hat. Aus diesem Grund dürfen Konten (z. B. für die Anmeldung am Arbeitsplatz oder in den notariellen Fachanwendungen) nicht geteilt werden, sondern jeder Nutzer muss, soweit technisch möglich und zweckmäßig, ein eigenes, personalisiertes Konto verwenden, das mit einem persönlichen und geheimen Passwort (vgl. hierzu Teil I Abschnitt 3.2) geschützt ist. Durch personalisierte Konten lässt sich zudem sicherstellen, dass Informationen nur von den jeweiligen Berechtigten eingesehen werden können und andere Nutzer nicht versehentlich wichtige Daten beschädigen oder löschen. Von der Zweckmäßigkeit ist daher regelmäßig auszugehen.

Umsetzung im Rahmen der notariellen Fachanwendungen

Jede Notarin und jeder Notar kann die Beschäftigten im Stammdatenverzeichnis der Bundesnotarkammer angeben. Die Beschäftigten werden insoweit der jeweiligen Amtsperson zugeordnet. Bei einer Sozietät kann eine Zuordnung auch zu den weiteren Amtspersonen erfolgen. Den Beschäftigten können gesonderte Rechte für den Zugang zu den Registern, XNP und weiteren Notarnetzdiensten zugeteilt werden, sodass diese jeweils ihre eigenen Zugangsdaten verwenden können. So erfolgt beispielsweise die Registrierung im ZTR über den jeweiligen Beschäftigten; jede Nutzung ist damit transparent nachvollziehbar. Die Berechtigungen sollten dabei stets auf dem aktuellsten Stand sein.

3.2 Passwortsicherheit

Passwörter sind Schlüssel, um auf eine bestimmte Ressource zugreifen zu können. Passwörter müssen, wie auch physische Schlüssel, immer über eine Mindestkomplexität verfügen.

Hinweis

Eine *Kombination* aus folgenden Kriterien trägt zu einer wesentlichen Verbesserung der Sicherheit bei:

- Ausreichende Länge (Mindestlänge von acht, idealerweise zwölf Zeichen)
- Buchstaben in Klein- und Großschreibung
- Zahlen und Sonderzeichen
- Nicht in einem Wörterbuch zu finden

Je länger das Passwort, desto schwieriger wird es sein, dieses zu erraten bzw. zu errechnen, z. B. durch einen „Brute Force"-Angriff. Bei diesem wird durch automatisiertes Ausprobieren aller denkbaren Kombinationen „mit Gewalt" versucht, das Passwort zu knacken. Mit steigender Komplexität wachsen die potentiellen Kombinationen exponentiell an, sodass ein Angriff deutlich mehr Zeit und Ressourcen erfordert.

Komplex bedeutet jedoch nicht kompliziert. Beispielsweise genügt es, einen Merksatz zu bauen:

Notarinnen & Notare arbeiten im Jahr 2022 mit sehr sensiblen Daten von vielen Bürgern!

Die ersten Buchstaben und Zeichen ergeben das Akronym *„N&NaiJ22mssDvvB!"*. Dieses Passwort ist – im Vergleich zu dem Passwort von Notarin Müller aus der Einleitung – entsprechend komplex und bedarf zur Einprägung nur eines einfachen Satzes.

Für verschiedene Anwendungen und Dienste (wie die Anmeldung zum Arbeitsplatzrechner, zur Notariatssoftware, zur Einsicht in das Grundbuch usw.) müssen für unterschiedliche Zugänge unterschiedliche Passwörter verwendet werden, ähnlich wie unterschiedliche Türen verschiedene Schlüssel erfordern. Auf diese Weise kann im Falle der Kompromittierung eines Passwortes ein Angreifer nicht gleichzeitig auf alle anderen Systeme und Informationen zugreifen. Es empfiehlt sich, einen Passwortmanager, der Passwörter nach dem Stand der Technik schützt, zu verwenden, um die unterschiedlichen Passwörter abzuspeichern. Besonders gefährdet sind Passwörter von Onlinediensten, insbesondere bei öffentlichen, nicht nur aus dem Notarnetz zugänglichen Diensten, sowie E-Mail-Konten.

Weiterhin müssen Passwörter bereits bei dem Verdacht der unbefugten Kenntniserlangung unverzüglich geändert werden – wie ein Türschloss bei einem Schlüsselverlust. Mittels eines sog. „Leak-Checkers“ kann überprüft werden, ob E-Mail-Adressen und zugehörige Passwörter durch ein Datenleck unberechtigt verbreitet wurden.

Voreingestellte Passwörter, z. B. das automatisch vergebene Passwort bei einer Erstanmeldung, müssen geändert werden. Passwörter sollten nicht automatisch im Browser gespeichert werden, da sie dort ungeschützt und außerdem bei einem defekten Rechner nicht mehr verfügbar sind.

Passwörter dürfen in keinem Fall weitergegeben oder in unmittelbarer Nähe des Endgerätes, z. B. unter der Tastatur, aufbewahrt werden. Wenn Passwörter dokumentiert werden, müssen diese sorgfältig und entsprechend geschützt aufbewahrt werden.

3.3 Mehr-Faktor-Authentisierung

Passwörter können – aller Schutzmaßnahmen zum Trotz – veröffentlicht, ausgelesen oder in sonstiger Weise kompromittiert werden. Durch eine Mehr-Faktor-Authentisierung können die daraus resultierenden Risiken minimiert werden. Dabei werden mindestens verschiedene zwei Faktoren kombiniert: Ein Faktor ist beispielsweise der physische Besitz einer Sache, in der Regel eines sog. „Tokens“ (z. B. ein Smartphone), der andere Faktor ist „Wissen“, in der Regel um ein Passwort oder eine PIN. Nur wer all diese Faktoren gleichzeitig zur Verfügung hat, erhält Zugang zum System oder zur Anwendung. Dieses Verfahren ist insbesondere vom Online-Banking (Stichwort „TAN-Generator“) bekannt.

Die Verwendung der Mehr-Faktor-Authentisierung empfiehlt sich insbesondere bei Cloud-Diensten. Aufgrund der Relevanz der dort abgespeicherten Daten sowie der Tatsache, dass die Seiten öffentlich verfügbar sind, also – anders als XNP – von Nutzern wie Angreifern gleichermaßen aufgerufen und Anmeldungen versucht werden können, stellen Cloud-Dienste ein interessantes Angriffsziel dar.

4. Aktualisierungen von Systemen

Nicht aktuell gehaltene Systeme beherbergen die Gefahr, dass (bekannte) Sicherheitslücken nicht geschlossen werden. Das sich stetig verändernde Gefahrenpotenzial erfordert eine regelmäßige Aktualisierung der Systeme. Von den Herstellern bereitgestellte Updates müssen daher eingespielt werden,

ähnlich einem Werkstattbesuch bei bekannten Fahrzeugmängeln. Dies betrifft die verwendete Software (Webbrowser) wie auch das Betriebssystem (Windows, MacOS, etc.) gleichermaßen.

5. Sichere Nutzung des Internets

Durch die große Anzahl internetbasierter Geschäftsprozesse gibt es eine mindestens ebenso große Bandbreite an möglichen Angriffen auf derartige Verfahren. Webseiten können beispielsweise so manipuliert werden, dass der Nutzer sich bereits bei deren bloßen Besuch mit Schadsoftware infiziert.

Daher ist beim Surfen im Internet Aufmerksamkeit gefragt. Dubiose und unseriöse Seiten sind meist bereits anhand ihres optischen Erscheinungsbildes (unprofessioneller Aufbau, Rechtschreib-/Grammatikfehler, fehlendes Impressum) zu identifizieren.

Weiterhin sollte beim Surfen immer auf eine verschlüsselte Verbindung geachtet werden, damit Angreifer bei der Eingabe von Daten nicht mitlesen können. Verschlüsselte Verbindungen können bereits anhand der Internetadresse – auch URL genannt – durch den Zusatz „https“ erkannt werden oder nach der Eingabe an einem kleinen Schlosssymbol in der Adressleiste des Browsers.

Zusätzliche Vorsicht und Zurückhaltung ist beim Download von Programmen und Dateien geboten. Ein Download sollte nur von vertrauenswürdigen offiziellen Seiten erfolgen. Es dürfen insbesondere keine Apps, Software und Dateien installiert oder heruntergeladen werden, die unaufgefordert per E-Mail zugesendet oder als Download-Link angeboten werden.

6. Zugang zu sensiblen Bereichen

Alle Geräte, insbesondere Arbeitsplatzrechner, Server oder Multifunktionsdrucker, sind durch organisatorische Maßnahmen (z. B. stetige Beobachtung oder geschützter Standort) vor unberechtigtem Zugriff zu schützen. Ihr Funktionieren kann organisationskritisch sein. Zudem enthalten diese Geräte meist sensible Informationen.

Arbeitsplatzrechner müssen blickgeschützt sein (z. B. durch Raumaufteilung, Aufstellung, Sichtschutzfolien). Die automatische Bildschirmsperre muss eingestellt sein. Darüber hinaus sollte der Bildschirm situationsabhängig auch bei einem kurzen Verlassen des Arbeitsplatzes manuell (z. B. durch die Tastenkombination Windowstaste + L) gesperrt werden, um sicherzustellen, dass niemand die auf dem Arbeitsplatzrechner gespeicherten Daten lesen, kopieren oder manipulieren kann.

7. Mobile Speichermedien

Mobile Speichermedien, insbesondere USB-Sticks, können sowohl zum Abgreifen von Daten als auch zum Einschleusen von Schadsoftware verwendet werden. Cyberkriminelle können mit Schadsoftware

präparierte USB-Geräte mit der Intention hinterlassen, dass diese gefunden und an einen Rechner angeschlossen werden. Unbekannte, aber auch privat angeschaffte Speichermedien dürfen daher im Netzwerk des Notarbüros nicht bzw. nur nach einer Überprüfung auf Schadsoftware durch einen in IT-Fragen kompetenten Beschäftigten oder den Systembetreuer verwendet werden. Der Einsatz individueller und einheitlicher USB-Sticks, die ausschließlich beruflich genutzt werden und das Notariat nicht verlassen dürfen, kann sich anbieten. Generell sollte das Speichern von Daten auf mobilen Speichermedien jedoch auf ein Mindestmaß reduziert werden.

8. Besonderheiten bei der Mobilarbeit

Mobiles Arbeiten ist in den vergangenen Jahren verstärkt in den Vordergrund gerückt. Aufgrund der situativen Besonderheiten ergeben sich hierdurch allerdings auch potentielle neue Gefahrenquellen, die spezifische organisatorische Maßnahmen erfordern.

Die VPN-Zugangsdaten (vgl. Teil II Abschnitt 12.1) müssen – wie auch Passwörter – blickgeschützt eingegeben werden und dürfen ebenfalls nicht weitergegeben werden. Gleichzeitig müssen Bildschirme bei einer Abwesenheit manuell gesperrt werden. Private Speichermedien dürfen auch hier nicht ungeprüft verwendet werden. Daten sollten nicht lokal, sondern auf Netzlaufwerken abgelegt werden, sodass sie auch im Falle des Geräteverlustes erreichbar sind und regelmäßig gesichert werden können.

Besonders sensible Daten sollten grundsätzlich nicht an öffentlichen Orten bearbeitet werden. Sollte dies ausnahmsweise erforderlich sind, müssen Smartphones, Tablets oder Laptops mit einer Sichtschutzfolie vor neugierigen Blicken geschützt sein. Darüber hinaus sollten IT-Geräte niemals unbeaufsichtigt liegen gelassen werden.

Zusätzlich sollte darauf geachtet werden, dass die PIN der SIM-Karte und der Bildschirmsperre des Mobiltelefons stets aktiviert ist. Die dabei verwendeten Zahlenkombinationen sollten nicht zu leicht zu erraten sein, insbesondere müssen logische Abfolgen wie 12345 vermieden werden. Alternativ besteht teilweise die Möglichkeit, Geräte per Fingerabdruck oder Gesichtserkennung zu entsperren. Beide Varianten bieten jeweils Vor- und Nachteile, sodass keine der jeweils anderen überlegen ist.

Apps sollten nur aus seriösen Quellen, d. h. offiziellen Stores wie dem AppStore oder Play Store bezogen werden, da das Gerät durch kompromittierende Software andernfalls beschädigt und Informationen unbemerkt abgerufen oder manipuliert werden können. Rooting und Jailbreaking, d. h. die Modifikation des Betriebssystems und das bewusste Umgehen systembedingter Sicherheitsmechanismen, sollten aus denselben Gründen unterbleiben.

Mobilgeräte sollten zum Aufladen und Übertragen von Daten nur an Kabel bzw. Rechner angeschlossen werden, denen vertraut wird. Durch die bloße Verbindung können bereits Schadprogramme übertragen oder Daten gestohlen bzw. manipuliert werden (vgl. hierzu Teil I Abschnitt 7).

Kurzüberblick Teil II

Teil II: Technische Erweiterung	
1. Identifizieren	
Wird die IT-Infrastruktur inventarisiert?	
Wird ein Netzwerkplan erstellt?	
2. Netzwerksicherheit	
Wird die Netzwerkintegrität durch eine Firewall geschützt?	
Werden deren Konfiguration und Regelwerk dokumentiert und regelmäßig überprüft?	
Werden wesentliche Netzwerkbereiche segmentiert?	
Wird auf die Nutzung von WLAN für Bürotätigkeiten verzichtet?	
Falls ein Verzicht nicht möglich ist: Werden die Besonderheiten beim Einsatz von WLAN beachtet? • Wird das WLAN nach dem Stand der Technik verschlüsselt? • Werden Gästezugänge vom internen Netz abgetrennt? • Werden Reichweite und Nutzbarkeit auf die nötigen Räume, Geräte und Beschäftigte beschränkt?	
3. Aktualisierung von Systemen	
Werden Sicherheitsupdates unverzüglich eingespielt?	
Werden Betriebssysteme zeitnah aktualisiert?	
Wird eine Patchmanagement-Software verwendet?	
4. Datensicherung und -wiederherstellung	
Existiert ein klares und strukturiertes Backup-Konzept? • Regelmäßige Durchführung • Verschlüsselung • Festlegung der Zuständigkeiten und der Verantwortlichen	
Werden Backups regelmäßig auf ihre Wiederherstellbarkeit getestet?	
Werden Cloud-Umgebungen für Backups verwendet? (siehe hierzu auch das Rundschreiben 04/21 der Bundesnotarkammer)	
Erfolgen zusätzliche Backups in einem anderen Brandabschnitt?	
5. E-Mail-Sicherheit	
Werden eingehende E-Mails bereits durch eine Software überprüft?	
Werden gefährliche (z. B. ausführbare) Dateianhänge automatisch blockiert?	
6. Endgeräteschutz	
Werden alle Endgeräte mit einer Endpoint-Protection-Lösung geschützt?	
Wird diese jeweils regelmäßig aktualisiert?	
7. Sichere Nutzung des Internets	
Werden webbasierte Inhalte, insbesondere der Inhalt und Code von Internetseiten, überprüft (z. B. durch Webfilter)?	
Existieren Regelungen zur privaten Nutzung der IT-Infrastruktur und werden diese regelmäßig überprüft?	

8. Verschlüsselung	
Werden erforderliche mobile Speichermedien und -geräte verschlüsselt?	
Werden sensible Informationen auf Fileservern verschlüsselt?	
Werden sensible Informationen auf Cloud-Plattformen verschlüsselt?	
9. Rollen- und Berechtigungskonzept	
Werden Berechtigungen aufgabenbezogen nach dem Prinzip der geringsten Berechtigung vergeben?	
Werden die vergebenen Rechte regelmäßig aktualisiert und ggf. entzogen?	
Existiert ein Rollenkonzept?	
10. Schutz sensibler Technik(bereiche)	
Sind Server, Datenspeicher und Netzwerkkomponenten vor unberechtigtem Zugriff und unbefugtem Zutritt geschützt?	
Werden die Schlüssel nur an bestimmte Beschäftigte ausgegeben?	
Wird der Zugang zu ausschließlichen Server- und Technikräumen protokolliert?	
Sind Arbeitsplatzrechner und Multifunktionsdrucker vor unberechtigtem Zugriff geschützt?	
Wird bei Multifunktionsdruckern ein Auslesen oder eine Firmwaremanipulation durch entsprechende Maßnahmen (z. B. durch Zugangskarten) verhindert?	
11. Notfallmanagement	
Existiert ein Notfallkonzept (z. B. Redundanz relevanter Systeme, Abschluss von Wartungsverträgen)?	
Wird von der „IT-Notfallkarte“ des BSI Gebrauch gemacht?	
12. Remote Zugriff	
Erfolgt die Absicherung des Fernzugriffs von Beschäftigten über einen VPN-Tunnel?	
Existieren klare Regeln und Maßnahmen zur Durchführung von Fernwartungen? (z. B. Verschlüsselung der Fernwartungsverbindung, Protokollierung der Verbindung)	
13. Entsorgung von Speichermedien	
Werden Speichermedien fachgerecht (durch Beachtung der DIN 66399 bei der Auswahl des Dienstleisters) entsorgt?	
14. E-Mail-Archivierung	
Werden E-Mails revisionssicher archiviert?	
Werden die archivierten E-Mails verschlüsselt?	
Können Systembetreuer nur mittels „Vier-Augen-Prinzip“ zugreifen?	
Werden Gateway-Lösungen zur Einhaltung von Löschfristen verwendet?	
15. Periodische Auditierung von Systemen	
Werden die Systeme periodisch auditiert und dokumentiert?	
Werden regelmäßig Penetrationstests durchgeführt?	
16. Logfilemanagement	
Existiert ein Logfilemanagement?	
Wurde die Tauglichkeit einer SIEM-Lösung geprüft?	

TEIL II – Technische Erweiterung

1. Identifizieren

Nur bei Kenntnis des Ist-Zustandes der eigenen IT(-Sicherheit) lässt sich der erwünschte Soll-Zustand erreichen. Zudem erleichtert und beschleunigt ein strukturierter Überblick den Austausch einzelner Komponenten im Falle eines Defekts. Daher sollten zunächst die für das Notarbüro erforderlichen Daten, Geräte und Systeme identifiziert und verwaltet werden. Hierunter fällt sowohl die Inventarisierung der physischen Geräte und Systeme als auch der genutzten Software und Anwendungen. Die Ressourcen werden dabei entsprechend ihrer Kritikalität und ihres Geschäftswerts priorisiert. Daneben sollte mittels eines Netzwerkplans eine grafische Übersicht der einzelnen Komponenten samt Abbildung der Datenflüsse bzw. Verbindungen zueinander vorgehalten werden.

2. Netzwerksicherheit

2.1 Firewall

Ein wesentliches Kernelement der IT-Sicherheit ist immer noch die zentrale Perimeter-Firewall. Sie regelt den Datenverkehr zwischen lokalem Netzwerk und dem Internet, also Fragen wie „Wer darf wie Datenverbindungen ins Internet aufbauen?“, „Welche Verbindungen ins interne Netzwerk sind zulässig?“ und „Welche Applikationen sind involviert?“.

Klassische Firewalls verfügen in der Regel über einen sehr großen Funktionsumfang wie Bandbreitenmanagement, Datenflusskontrolle, dynamisches Routing, Hochverfügbarkeit und VPN-Unterstützung. Vielfach sind Managementsysteme für die Verwaltung mehrerer Firewalls an verschiedenen Standorten inkludiert. Firewalls sind stets aktuell zu halten. Das Einspielen der Sicherheitsupdates der Hersteller (siehe hierzu vertiefend Teil II Abschnitt 3) ist Grundvoraussetzung für die Funktion und Sicherheit.

Ebenso wichtig ist es, die Konfiguration der Systeme stets zu prüfen und an die jeweiligen, sich ändernden Bedürfnisse anzupassen. Sämtliche Anpassungen am Regelwerk und an der Konfiguration müssen jeweils zeitnah, ausführlich und revisionssicher dokumentiert werden. Dies umfasst auch Änderungen, die im laufenden Betrieb vorgenommen werden. Dabei sind nicht (mehr) erforderliche Regeln zu streichen, um zu vermeiden, dass die Regelwerke ohne Prüfung ihrer Aktualität oder Sinnhaftigkeit über viele Jahre anwachsen.

2.2 Netzwerksegmentierung

Innerhalb eines Netzwerkes müssen wesentliche Bereiche voneinander getrennt und abgesichert werden. Es sollte mindestens zwischen internem und externem Netz separiert werden, idealerweise werden jedoch drei Sicherheitszonen eingerichtet:

- Internes Netz für notarielle Fachanwendungen wie z. B. XNP, ZTR, ZVR
- Demilitarisierte Zone (DMZ) für den Mail-Server und die Webseite des Notarbüros, insbesondere wenn diese Webanwendungen zur Kontaktaufnahme oder Terminvereinbarungen vorhält
- Externes Netz (WAN) für den sonstigen Datenverkehr

Die Zonenübergänge müssen dabei durch eine Firewall separiert und geschützt werden. Der Datentransfer zwischen den Zonen muss basierend auf einem adäquaten Regelwerk analysiert und eingeschränkt werden. Es soll ausschließlich erlaubte Kommunikation weitergeleitet werden.

Zusätzlich müssen Gastzugänge – soweit diese nicht über einen separaten Router eingerichtet werden – und Netzbereiche, in denen keine ausreichende interne Kontrolle über die Endgeräte gegeben ist, in unterschiedliche Netzsegmente platziert werden. Innerhalb des Serversegments kann nochmals eine Unterteilung erfolgen, z. B. jeweils ein Netzwerksegment für Backups, für Datenbankserver oder einen oder mehrere Clients. So wird kontrolliert, wer auf welche Ressourcen zugreifen kann bzw. darf, und die Angriffsfläche möglichst reduziert. Die Verbreitung von Schadsoftware und die Möglichkeiten der Angreifer können so eingedämmt werden.

2.3 WLAN

Auf die Nutzung eines WLAN für Bürotätigkeiten sollte verzichtet werden. Sofern die Nutzung erforderlich sein sollte, ist dieses nach dem Stand der Technik zu verschlüsseln. Falls ein Gäste-WLAN angeboten wird, muss auf eine strikte Trennung zwischen diesem und dem internen Netz geachtet werden. Auch die Reichweite und Nutzbarkeit des WLAN sollten auf die erforderlichen Räume, Endgeräte und Beschäftigten beschränkt werden.

3. Aktualisierungen von Systemen

Wenn Sicherheitsupdates für Software zur Verfügung stehen, sollten diese unverzüglich installiert werden. Angaben zum Lebenszyklus unterschiedlicher Windowssysteme können unter https://docs.microsoft.com/de-de/lifecycle/products/ abgerufen werden. Hierbei ist zu beachten, dass der Lebenszyklus lediglich Aufschluss darüber gibt, ob das Produkt von Seiten des Herstellers überhaupt noch unterstützt wird. In vielen Fällen erfolgen jedoch bereits zuvor keine relevanten Sicherheitsupdates mehr. Da der Hersteller seinen Fokus auf das jeweils aktuellste Produkt legen dürfte, sollten insbesondere Betriebssysteme daher regelmäßig deutlich früher auf ein aktuelles System umgestellt werden.

Dadurch können einerseits die neuen Funktionalitäten genutzt werden. Andererseits wird ausgeschlossen, dass es gegebenenfalls zu technisch bedingten Lücken in den Sicherheitsupdates des Altsystems kommt. In Fällen, in denen dies beispielsweise aus Kompatibilitätsgründen nicht möglich ist, sollte der Einsatz von Workarounds geprüft werden, die die Ausnutzung einer Schwachstelle verhindern. In Situationen, in denen weder Sicherheitsupdates noch funktionierende Behelfslösungen vorhanden sind, sollte eine vorübergehende Abschaltung der betroffenen Software erwogen werden.

Zur Erleichterung des Patchmanagements kann eine geeignete Software wie WSUS eingesetzt werden.

Hinweis

Windows XP, 7, Vista und 8 sowie macOS Sierra und High Sierra sind Beispiele für veraltete Betriebssysteme, welche nicht mehr verwendet werden dürfen. Diese erhalten keine Updates mehr. Im Falle von Windows 10 kann in den Einstellungen nach tagesaktuellen Updates gesucht werden. Diese müssen installiert und dürfen nicht ignoriert werden.

---

4. Datensicherung und -wiederherstellung

Eine Datensicherung (Backup) wird idealerweise selten bis nie benötigt, ist in kritischen Situationen wie einem technischen, menschlichen oder durch äußerliche Einflüsse bedingten Versagen jedoch essentiell. Obgleich Backups nur ausnahmsweise relevant werden, darf insoweit keine Nachlässigkeit entstehen.

Deshalb ist es notwendig, Sicherungen umfassend zu planen und regelmäßig zu überprüfen, ob eine Rücksicherung möglich ist. Es ist notwendig, nicht nur Daten, sondern auch wichtige Systeme zu sichern. Die Art und Weise, wie die Datensicherung erfolgt, ist abhängig von der Bedeutung des gesicherten Systems und von der Menge der zu schützenden Daten.

Zusätzlich müssen sowohl die Zuständigkeiten als auch deren Vertretungen für das Backup geregelt werden. Nur so kann sichergestellt werden, dass diese mit der nötigen Sorgfalt durchgeführt werden.

Hinweis

Es ist nicht nur wichtig, Backups durchzuführen und auf Vollständigkeit und Korrektheit zu untersuchen, sondern diese auch in regelmäßigen Abständen auf Wiederherstellbarkeit zu prüfen und das fehlerfreie Einspielen zu testen. Dabei sollten die Datensicherungen auf verschiedenen Speichermedien erfolgen und an verschiedene Orte platziert werden (z. B. anderer Brandabschnitt, Tresor, außerhalb des Netzwerkes), um vor Diebstahl, Brand oder auch Wasserschäden geschützt zu sein.

Es existieren drei Arten der Datensicherung: Volldatensicherung, inkrementelle und differenzielle Datensicherung. Bei der Entscheidung, welche Datensicherungsstrategie angewendet werden soll, sind einige Faktoren zu berücksichtigen, unter anderem die zugrundliegenden Verfügbarkeitsanforderungen oder auch die Änderungszeitpunkte der Daten. Existieren z. B. Zeitpunkte, an denen anwendungsbezogen der Komplettdatenbestand gesichert werden muss (z. B. nach buchhalterischen Wochen-, Monats- oder Jahresabschlüssen), so kommt zu diesen Zeitpunkten eine Vollsicherung infrage.

Im Falle eines Datenverlustes sind alle Daten bis zur letzten Sicherung verloren. Je aktueller die letzte Datensicherung ist, desto weniger Verlust ist zu verkraften. Auch hier ist zu betrachten, wie hoch der Wiederherstellungsaufwand ohne Datensicherung und das Änderungsvolumen ist. Der zeitliche Abstand der Datensicherungen ist so zu wählen, dass die Restaurierungs- und Nacherfassungszeit der in einem gewissen Zeitraum geänderten Daten kleiner als die maximal tolerierbare Ausfallzeit ist. Ebenso sollten Zeitpunkte betrachtet werden, an denen sich die Daten in großem Umfang ändern oder an denen der Komplettdatenbestand vorliegen muss.

Grundsätzlich sollten Datensicherungsmedien und Originaldatenträger in unterschiedlichen Brandabschnitten aufbewahrt werden und nur berechtigten Personen zugänglich gemacht werden; die Nutzung einer Cloud-Umgebung kann sich insoweit anbieten. Vertrauliche Daten sollten vor der Sicherung möglichst verschlüsselt werden, wobei darauf geachtet werden muss, dass eine Entschlüsselung auch nach einem längeren Zeitraum möglich ist.

5. E-Mail-Sicherheit

Nach wie vor ist die E-Mail das wesentliche Einfallstor für Angriffe aller Art. Daher sollte grundsätzlich eine zentrale E-Mail-Sicherheitslösung genutzt werden. Gesendete und empfangene E-Mails können so automatisiert hinsichtlich ihrer Vertrauenswürdigkeit analysiert und gegebenenfalls blockiert werden. Das ermöglicht den nachhaltigen Schutz vor unerwünschten E-Mails. Bestimmte Dateianhänge wie z. B. exe-Dateien sollten grundsätzlich blockiert werden.

6. Endgeräteschutz

Zentraler Baustein für das IT-Sicherheitsniveau ist der flächendeckende Einsatz einer modernen Endpoint-Protection-Lösung, umgangssprachlich auch Antiviren-Software genannt, obgleich Letztere nur einen Teilbereich der Endpoint-Protection darstellt.

In der Vergangenheit wurde die Infektion mit Schadsoftware oftmals erst nach mehreren Wochen oder Monaten bemerkt, da klassische Antivirenprogramme lediglich auf Signaturen und Heuristiken basieren. Dies bedeutet, dass sie nur bereits bekannte Schadsoftware erkennen können. Moderne Lösungen setzen dagegen auf eine Vielzahl von Methoden. Anhand ihres Verhaltens und der von ihr aufgebauten Netzwerkverbindungen sowie mit Hilfe von Künstlicher Intelligenz kann zwischen „guter“ und „bösar-

tiger“ Software unterschieden werden. Darüber hinaus bieten moderne Endpoint-Protection-Lösungen weitergehende Module zum Schutz vor gefährlichen Webinhalten und zur Kontrolle von Schnittstellen.

7. Sichere Nutzung des Internets

Durch die Zunahme webbasierter Prozesse ist das Internet in den Fokus betrügerischer und kompromittierender Angriffe gerückt. Gefälschte Webseiten und manipulierte Applikationen sind nur zwei Beispiele von vielen.

Der Einsatz von Webfiltern und intelligenten Technologien, die die Vertrauenswürdigkeit von webbasierten Inhalten prüfen und gewährleisten, müssen ein fester Bestandteil einer IT-Sicherheitsstrategie sein. Der Inhalt von Webseiten und deren Code sollten genauestens analysiert werden. Wesentlich sind in diesem Zusammenhang auch die Überprüfung und Analyse der von den Nutzern verwendeten webbasierten Applikationen (z. B. kostenlose Übersetzungsprogramme). Es macht häufig einen großen Unterschied, ob derartige Applikationen mit einer gültigen Lizenz verwendet werden oder als kostenlose (Test-)Version. Letzteres bedeutet zudem häufig, dass das Recht an den dort abgelegten, verarbeiteten oder geteilten Informationen aufgegeben wird.

Daneben sollten Regeln bezüglich der privaten Nutzung der dienstlichen IT-Infrastruktur, insbesondere bei der E-Mail- und Internetnutzung, entwickelt werden. Die Regeln müssen klar und deutlich definiert, dokumentiert und stichprobenartig – zur Vermeidung einer abweichenden betrieblichen Übung – auf ihre Einhaltung überprüft werden.

8. Verschlüsselung

Verschlüsselungstechnologien haben viele Einsatzbereiche, bezwecken jedoch maßgeblich den Schutz mobiler Datenträger, besonderer Informationen im Netzwerk (z. B. Personal- oder Beteiligtendaten), oder der Datenkommunikation (z. B. über E-Mail). Verschlüsselungstechnologien müssen trotz der komplexen Technik im Hintergrund für die Nutzer praktikabel und handhabbar sein.

Verschlüsselung

Verschlüsselung bedeutet, dass ein klar lesbarer Text mittels kryptographischer Verfahren in einen „Geheimtext“ umgewandelt wird und nur mittels eines Schlüssels wieder lesbar gemacht werden kann. Verschlüsselung kombiniert ein mathematisches Verfahren (den Verschlüsselungsalgorithmus) mit einem Schlüsselwort (Kennwort, Passwort, „Passwortsatz“ oder Kombination von Zeichen, Näheres hierzu in Teil I Abschnitt 3.2).

Wegen des Verlust- und Diebstahlrisikos müssen erforderliche mobile Speichermedien und -geräte (z. B. Notebooks, Tablets, Smartphones, USB-Sticks, externe Festplatten), die die Geschäftsstelle verlassen, nach dem Stand der Technik verschlüsselt werden.

Mobile Device Management

Smartphones sind mittlerweile umfangreiche Datenträger mit Zugriff auf die Organisationsinfrastruktur geworden. Soweit sich auf den – insbesondere von Beschäftigten – betrieblich verwendeten Geräten kritische Daten befinden, sollte deren Verarbeitung transparent und sicher erfolgen.

Dies kann durch ein Mobile Device Management ermöglicht werden. Hierdurch können den Nutzern E-Mail-Konten zugewiesen, Geräte mit den Compliance-Vorgaben abgeglichen sowie gewünschte Apps auf die Geräte übertragen oder unerwünschte Apps verboten werden. Ferner ist nachvollziehbar, welche Daten sich auf dem Gerät befinden bzw. befunden haben. Daneben besteht die Möglichkeit einer Löschung durch Fernzugriff bei Verlust oder Diebstahl. Einige Lösungen bieten zudem eine Container-Funktion zur vollständigen Trennung privater und geschäftlicher Daten auf dem Gerät.

Neben den Datenträgern und Geräten wird empfohlen, auch sensible Informationen auf Fileservern und in der Cloud zu verschlüsseln und nur für autorisierte Personen zugänglich zu machen. Hierbei sollte darauf geachtet werden, dass verschlüsselte Daten im Bedarfsfall verlässlich entschlüsselt werden können. Wichtig ist – insbesondere in Hinblick auf den Fileserver –, dass die Verschlüsselung die Arbeit der Nutzer nicht über Gebühr erschwert. Die Technologien müssen sich nahtlos in das IT-System des Notarbüros einfügen, sie müssen kostensparend, zentral zu verwalten und zu verteilen sein. Sollte hiernach eine Verschlüsselung in Betracht kommen, sollte sie auch eingesetzt werden. Vorteilhaft sind hier Systeme, die im Hintergrund und aufgrund technologischer Gegebenheiten zwingend für eine Verschlüsselung sorgen, sodass diese automatisiert erfolgt und nicht vergessen werden kann.

9. Rollen- und Berechtigungskonzept

Die IT-Systeme einer Organisation beherbergen vielzählige Daten. Durch ein Identitäts- und Berechtigungsmanagement wird festgelegt, ob und in welcher Granularität Informationen oder Dienste genutzt werden dürfen. Dadurch wird sichergestellt, dass den Nutzern nur die notwendigen Berechtigungen zugeordnet werden. Je nach ihrer Rolle wird ihnen der Zugriff gewährt oder verweigert. Berechtigungen dürfen nur eingeschränkt und aufgabenbezogen nach dem Prinzip der geringsten Berechtigung eingerichtet werden. So benötigen ausschließlich für gesellschaftsrechtliche Vorgänge zuständige Sachbearbeiter meist keinen Zugriff auf das ZVR oder ZTR. Die Zuordnung ist regelmäßig zu überprüfen und gegebenenfalls anzupassen.

Damit der Überblick über die Zugriffsberechtigungen der Nutzer nicht verloren geht, empfiehlt es sich, ein Rollenkonzept zu erstellen. Die unterschiedlichen Berechtigungen werden dabei je nach Prozess in entsprechende Rollen zusammengefasst. Durch die Definitionen von Rollen für gleiche Aufgaben können die Berechtigungen zentral und effizient verwaltet werden.

10. Schutz sensibler Technik(bereiche)

Sensible Geräte, insbesondere Server, Datenspeicher und Netzwerkkomponenten, und die zugehörigen Räumlichkeiten sind durch entsprechende organisatorische Maßnahmen (z. B. durch Gestaltung/Aufteilung/Schutz der Räumlichkeiten, Platzierung der Geräte, manuelle Freigabe) vor unbefugtem Zugriff bzw. unberechtigtem Zutritt zu sichern. Schlüssel sollten nur bestimmten Beschäftigten ausgehändigt werden. In einem ausschließlich genutzten Server- und Technikraum kann sich eine Protokollierung der jeweiligen Person und des Zeitraums des Aufenthalts anbieten. Arbeitsplatzrechner und Multifunktionsdrucker sind ebenfalls zu schützen, insbesondere um manipulative Eingriffe in das Netzwerk auszuschließen. Ein Auslesen der Daten des Druckers oder die Manipulation der Firmware sollte beispielsweise mittels Zugangskarte/-token oder PIN-Eingabe verhindert werden.

11. Notfallmanagement

Ausnahmesituationen wie Stromausfälle oder der Ausfall von IT-Kühlanlagen oder Datenverbindungen können den reibungslosen IT-Betrieb erheblich gefährden. Vorausschauendes Sicherheitsmanagement bedeutet, sich auch gegen derartige Vorfälle zu wappnen. Notfallmaßnahmen sollten in Form eines Notfallkonzepts ausgearbeitet sein. Dieses umfasst Handlungsschritte für die Wiederherstellung der Geschäftsprozesse oder wichtiger Ressourcen, deren Priorisierung sowie die jeweiligen Zuständigkeiten. Dabei sind nicht nur die Antwort-, sondern auch die Lösungszeiten im Falle eines Vorfalls festzulegen. Zusätzlich kann der Einsatz der „IT-Notfallkarte“ des BSI das Notfallmanagement erleichtern.[1]

Eine weitere Internetanbindung über LTE oder 5G sichert die Aufrechterhaltung aller extern genutzten Datenanbindungen. Einem Stromausfall und einem damit einhergehenden Datenverlust kann durch eine unterbrechungsfreie Stromversorgung basierend auf Batterien begegnet werden. Der Abschluss von Wartungsverträgen gewährleistet einen schnellen Austausch bei Hardwaredefekten.

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html.

12. Remote Zugriff

Ein Fernzugriff auf interne Ressourcen kann aus unterschiedlichen Gründen sinnvoll und notwendig sein, beispielsweise zur externen Administration interner Systeme oder für einen Zugriff aus dem Homeoffice auf intern abgelegte Dokumente. Der externe Zugang ist dabei abzusichern.

12.1 Homeoffice

Ein externer Zugriff auf netzinterne Ressourcen sollte über eine VPN-Verbindung erfolgen.

Grundsätzlich existieren zwei Möglichkeiten, wie derartige Zugänge realisiert werden können. Sicherer ist es dabei, wenn jeglicher Datenverkehr über den VPN-Tunnel übertragen wird. Dies gilt insbesondere auch für Zugriffe auf Webseiten und Daten im Internet. Somit kann gewährleistet werden, dass die zentral etablierten Schutzmechanismen wie Webfilter auch für diese Nutzer und Geräte zum Einsatz kommen. Das Schutzniveau bleibt für interne wie externe Nutzer gleich. Jedoch gibt es technische Gründe, wie beispielsweise eine schwache Internetanbindung, die einen Zugriff auf Ressourcen im Internet direkt vom Gerät erfordern. Derartige direkte Verbindungen im Rahmen des sog. „Splittunneling“ erfordern ein hohes Augenmerk bezüglich des Schutzes des jeweiligen Endgerätes, da an dieser Stelle zentral-etablierte Schutzmechanismen nicht greifen können.

12.2 Fernwartung

Falls externe Dienstleister oder eigene Systembetreuer zur Durchführung einer Fernwartung auf die interne IT-Infrastruktur zugreifen, ist einem Missbrauch der Fernwartungsverbindung (von dritter Seite) durch entsprechende Maßnahmen vorzubeugen. Es bietet sich insoweit an, nur die für die Ausführung der Tätigkeit relevanten Zugriffsrechte zu erteilen sowie den Zugriff zeitlich zu begrenzen und nur für die konkreten Aufgaben explizit zu erlauben. Daneben sollten die Fernwartungsverbindungen verschlüsselt sein und derartige Verbindungen wie auch die erfolgten Tätigkeiten protokolliert werden.

13. Entsorgung von Speichermedien

Speichermedien müssen fachgerecht entsorgt und vernichtet werden, um einen unberechtigten Zugriff auf die gespeicherten Daten zu vermeiden. Dazu zählen jegliche Speichermedien aus Servern, Switches, Notebooks, Druckern usw., auch wenn diese (vermeintlich) defekt sind. Dabei sind die DIN-Norm 66399 und die dazugehörige Schutzklassenzuordnung als auch Datenträger-Vernichtungsempfehlungen bei der Auswahl des Dienstleisters zu beachten.

14. E-Mail-Archivierung

Soweit Geschäftsprozesse und -kommunikation per E-Mail abgewickelt werden, müssen diese revisionssicher über die Dauer der Aufbewahrungspflicht archiviert werden. Hierfür relevante gesetzliche Vorgaben sind beispielsweise die Anforderungen an eine lückenlose Dokumentation von steuerrelevanten Daten (siehe u. a. AO, BGB, HGB, GoBD) oder an die Nebenakten (§§ 50 Abs. 1 Nr. 7, 52 NotAktVV). E-Mail-Archivierung bedeutet auch, dass diese jederzeit mit angemessenem Aufwand durchsucht und dem Berechtigten zur Verfügung gestellt werden können.

Grundsätzlich basieren moderne E-Mail-Archivierungskonzepte auf einer zentralen serverbasierten Archivierung. Nur so kann sichergestellt werden, dass interne und externe E-Mails revisionssicher archiviert werden und ein ordnungsgemäßer Nachweis des E-Mail-Verkehrs ermöglicht wird. Die E-Mails sollten zudem verschlüsselt abgelegt werden und ein Zugriff des Systembetreuers nur auf Basis eines Vier-Augen-Prinzips erfolgen. Die einzuhaltenden Löschfristen können durch eine Gateway-Lösung für bestimmte Postfächer automatisiert gehandhabt werden.

15. Periodische Auditierungen von Systemen

Es wird empfohlen, eine regelmäßige Auditierung der Systeme durchzuführen und dies – insbesondere mit Blick auf die DS-GVO – zu dokumentieren. Solche Audits prüfen vorhandene Prozesse, Regeln und auch die dahinterstehenden organisatorischen Vorkehrungen. So können sich für die Weiterentwicklung der IT-Sicherheit wertvolle Erkenntnisse ergeben und die Wirksamkeit sichergestellt werden.

Weiterhin können durch sog. „Penetrationstest“ – einer Simulation potentieller Angriffe unter kontrollierten Bedingungen – etwaige Schwachstellen und Lücken aufgedeckt werden, welche von unnötig geöffneten Ports (*Vulnerability Scan*) bis hin zu unaufmerksamen Beschäftigten reichen.

16. Logfilemanagement

Logfiles dienen grundsätzlich der Nachvollziehbarkeit und Beurteilung von Sicherheitsvorfällen und bieten die Möglichkeit, Gefahrenpunkte und Angriffe frühzeitig zu erkennen. Da IT-Systeme jedoch eine Vielzahl an Logdateien („Events“) erzeugen, kann sich in größeren Notarbüros der Einsatz von zentralen Logfilemanagement-Lösungen anbieten, um eine maschinelle Analyse und Auswertung der Events zu ermöglichen. Da Logfiles aus den unterschiedlichsten Quellen (z. B. Firewall, Datenbanksystemen, Servern) stammen, gilt es, diese nicht nur zu sammeln, sondern in schnell verwertbarer Form aufzubereiten. Hierfür können sich Security Incident & Event Management Lösungen (SIEM) anbieten. Diese fungieren als Alarmzentrale, die aus den gesammelten und analysierten Daten mit Hilfe intelligenter Suchalgorithmen Zusammenhänge zwischen unterschiedlichen Ereignissen herstellen können.

Fazit

So umfassend die Angriffsmöglichkeiten sind, so umfassend kann ihnen begegnet werden. Trotz zunehmender Digitalisierung und sich ändernder Prozesse bzw. Technologien trägt nach wie vor die Beachtung der Grundregeln der IT-Sicherheit bereits zu einer erheblichen Steigerung des Schutzniveaus im Notariat bei. So können Angriffe, wie sie Frau Dr. Müller erfahren musste, verhindert oder jedenfalls wesentlich erschwert werden. Ein hohes IT-Sicherheitsniveau lässt sich allerdings nicht ad hoc erreichen, sondern erfordert einen kontinuierlichen Prozess. Jede Notarstelle muss für seine individuellen Bedürfnisse, die eigene IT-Landschaft und die konkreten Anforderungen die richtigen Technologien finden, erproben und einsetzen. Dies erfordert die Entwicklung von klaren Strategien und daraus abgeleiteten Konzepten unter Berücksichtigung zur Verfügung stehender Ressourcen.

Wie sich insbesondere im ersten Teil dieser Handreichung zeigt, stellt der „Faktor Mensch“ ein entscheidendes Element im Bereich der IT-Sicherheit dar. Notarinnen und Notare, Beschäftigte und deren Kenntnisse, Verhaltensweisen und Aufgaben sollten ein maßgeblicher Bestandteil des Sicherheitskonzepts sein. Das Bewusstsein für IT-Sicherheit muss bei allen Nutzerinnen und Nutzern nicht nur geweckt, sondern auch wachgehalten werden.