Sicherheitsrichtlinien

1. Grundlagen

1.1. Das von der NotarNet GmbH betriebene Notarnetz bietet eine sichere Kommunikationsinfrastruktur für Notare, ihre Büros und ihre Berufsorganisationen auf dem jeweiligen Stand der Technik. Ziel der Einrichtung ist es, Notaren einen sicheren Zugang zum Internet sowie einen geschlossenen eigenen Kommunikationsbereich bereitzustellen. Die Dienste, Daten und Anwendungen des Notarnetzes werden in einem sicheren Rechenzentrum betrieben und gepflegt. Über das Notarnetz sind das Zentrale Testamentsregister und das Zentrale Vorsorgeregister der Bundesnotarkammer („Zentrale Register“) unmittelbar erreichbar.

1.2. Die implementierten technischen Sicherheitsmaßnahmen können nur dann einen wirksamen Schutz bieten, wenn jeder Teilnehmer diese Sicherheitsrichtlinien umfassend berücksichtigt und befolgt. Dies dient der Einhaltung der notariellen Verschwiegenheitspflicht, dem eigenen Schutz, dem anderer Nutzer und insbesondere der Sicherheit der Zentralen Register.

1.3. Neben den technischen Einrichtungen des Notarnetzes gehören zu einer kompletten Absicherung auch technische Maßnahmen in den lokalen Systemen und organisatorische Maßnahmen in der Notarstelle. Durch den Anschluss an das Notarnetz ist der Notar verpflichtet, die lokale Sicherheit für den Betrieb des Notarnetzes und der Zentralen Register zu gewährleisten.

1.4. Mit dem sog. IT-Grundschutz hat das BSI (Bundesamt für Sicherheit in der Informationstechnik) eine Methodik für ein effektives, alle Schutzbereiche umfassendes IT-Sicherheitsmanagement entwickelt. Das Notarnetz, seine technischen und organisatorischen Einrichtungen und die konzeptionellen Empfehlungen werden an dieser Methodik ausgerichtet. Weitergehende Informationen, Hintergründe und Erläuterungen entnehmen Sie bitte den Internetseiten des BSI (www.bsi.de, www.bsi-fuer-buerger.de).

1.5. Die vorliegenden Sicherheitsrichtlinien stellen auf den jeweiligen Stand von Recht und Technik ab. Sie werden bei sich ändernden rechtlichen und/oder technischen Rahmenbedingungen im Interesse aller Nutzer entsprechend angepasst.

2. Richtlinien für die lokale Sicherheit

2.1. Auf jedem an das Notarnetz angeschlossenen PC ist ein zuverlässiges Viren-Schutzprogramm einzusetzen. Dieses dient zur Überprüfung von Daten, die verschlüsselt übertragen und erst beim Empfänger im lokalen System entschlüsselt werden. Auch Daten, die über andere Medien (bspw. USB-Stick, MP3-Player, CD, DVD) auf das System gelangen, werden hiermit überprüft.

2.2. Durch eine zusätzliche Versorgung der angeschlossenen Computer und Programme mit regelmäßigen Sicherheitsupdates (Virenschutz und andere sicherheitsrelevante Komponenten, Betriebssysteme und Anwendungs-Programme) werden die jeweils neu entdeckten Sicherheitslücken geschlossen. Solche Aktualisierungen für alle sicherheitsrelevanten Komponenten sind unerlässlich. Beim Virenschutz hat die Aktualisierung der Virendefinitionsdateien mindestens einmal pro Arbeitstag zu erfolgen.

2.3. Eine regelmäßige Untersuchung aller Systeme auf das Vorhandensein von sog. Keyloggern (Schadsoftware, die durch die Protokollierung von Tastatureingaben dem Ausspionieren von Benutzernamen und Passwörtern dient) und sog. Botnets (Programme, die den betroffenen Computer mit einem Netz anderer Computer zusammenschließen und so Attacken mit erheblicher Rechenleistung auf vordefinierte Ziele führen) ist durchzuführen.

2.4. In jeden Fall müssen alle wichtigen Daten mit einer geeigneten Datensicherungseinrichtung regelmäßig gesichert werden, um notfalls infizierte oder nicht mehr zugreifbare Daten auf möglichst aktuellem Stand wieder herstellen zu können. Dabei sind die gängigen Empfehlungen für die Datensicherung zu beachten. Durch geeignete Maßnahmen muss verhindert werden, das Schadsoftware auch den Inhalt des Datensicherungs-Medium befällt. Überprüfen Sie regelmäßig, ob auch tatsächlich alle Daten gesichert werden und diese auch wiederherstellbar sind.

2.5. Außer für den Login im Notarportal und den Zentralen Registern fragen Bundesnotarkammer und NotarNet GmbH Benutzername und Passwort nicht ab. Solche Login-Mechanismen der Bundesnotarkammer sind stets SSL-gesichert. Dies ist erkennbar an der mit „https“ beginnenden Adresse im Browser und der farbig (in der Regel grün) markierten Adressleiste, über welche der Aussteller des SSL-Zertifikats ermittelt werden kann. In Zweifelsfällen sollte eine Eingabe von Benutzername und Passwort unterbleiben und der Notarnetz-Support eingeschaltet werden. Grundsätzlich ist bei der Zusendung von harmlos aussehenden Links per E-Mail die notwendige Vorsicht geboten. Hierhinter kann sich auch ein auf eine schadhafte Drittseite, die den Seiten der Bundesnotarkammer ähnlich sieht, zeigender Link verbergen, welcher nur den Sinn hat, die Benutzerdaten auszuspähen (sog. Phishing-Verfahren).

2.6. Weitere Risiken können eingedämmt werden, wenn in den lokalen Einstellungen für den Internet-Browser die Ausführbarkeit von ActiveX auf den Arbeitsplätzen nur nach vorheriger Zustimmung des Benutzers möglich oder sogar deaktiviert ist. Für Java und Javascript kann die Ausführbarkeit auf vertrauenswürdige Internetseiten beschränkt werden. Zu den vertrauenswürdigen Seiten sind auf jeden Fall diejenigen der Bundesnotarkammer und der NotarNet GmbH hinzuzufügen.

2.7. Um das Ausführen oder Nachladen von Schadcode beim Öffnen oder Bearbeiten von Office-Dateien, wie z.B. Worddokumenten zu vermeiden, aktivieren Sie bitte die Sicherheitseinstellungen im Sicherheitscenter aller Microsoft-Office-Programme wie beispielsweise die Makrosicherheit in Microsoft Word. Achten Sie bei der Verwendung anderer Programme auf entsprechende Einstellungen und Sicherheitsempfehlungen.

2.8. Der Systembetreuer wartet die lokalen Sicherheitseinrichtungen und weist Verantwortliche im Büro in einfache Überwachungsaufgaben wichtiger Funktionen ein. Ein Notfallplan mit den wichtigsten Kontaktadressen und Informationen zu den technischen Einrichtungen sollte bereit liegen.

2.9. Eine Fernwartung für erforderliche Wartungsarbeiten sollte für Softwarehäuser oder Systembetreuer nur im Bedarfsfall und nur vorübergehend aktiviert werden. Die Remote-Einwahl sollte in jedem Fall verschlüsselt erfolgen, vom Notar initiiert werden und jederzeit vom Notar unterbrochen werden können. Im Übrigen wird auf die EDV-Empfehlungen für Notarinnen und Notare, Notarprüferinnen und Notarprüfer und Softwarehersteller im Hinblick auf eine dienstordnungsgerechte Führung der Bücher, Verzeichnisse und Übersichten im Notariat der Bundesnotarkammer (Stand: Mai 2005) hingewiesen.

2.10. Notebooks und andere mobile Geräte, die an fremde Netze oder Internetzugänge angeschlossen werden (WLAN-

Hotspots, fremde Firmen- oder Privatnetzwerke, o.ä.) können als Überträger von Schadprogrammen dienen und sollten daher anschließend nur nach sorgfältiger Sicherheits-Überprüfung wieder mit dem Büro-Netzwerk verbunden werden.

2.11. Bei mobilen Geräten mit Notarnetz-Mobilzugang muss die Geräte-Nutzung durch PIN- bzw. Passwort-Freigabe geschützt werden, außerdem muss eine Bildschirmsperre mit PIN-Freigabe eingestellt werden. Dies beugt in erster Linie einem Missbrauch der Daten und Datenverbindungen vor, wenn das Gerät durch Unvorsichtigkeit oder Verlust in falsche Hände gerät. Außerdem ist eine Verschlüsselung des Gerätespeichers zu empfehlen sowie eine sorgfältige Prüfung vor der Installation von Apps hinsichtlich deren Vertrauenswürdigkeit. Viele harmlos aussehende Apps sammeln im Hintergrund unbemerkt Daten aller Art und übermitteln sie versteckt per Internetverbindung.

2.12. Beim Einsatz von Funknetzwerken (WLAN) müssen geeignete Sicherheitsmaßnahmen ergriffen werden. Als unsicher gelten unter anderem solche Funknetzwerke, die zum Schutz sog. „WEP-Verschlüsselung“ (Wired Equivalent Privacy) einsetzen. Zur Sicherung eines angeschlossenen Funknetzwerks ist mindestens die sog. „WPA-2-Verschlüsselung“ mit Benutzername und einem kryptischen aus Buchstaben, Zahlen und Sonderzeichen bestehenden sowie mindestens 10 Zeichen langen Passwort oder ein technisch fortgeschritteneres Verfahren zu verwenden. Die Identität des Netzwerks („SSID“) darf nicht offen übermittelt werden. Insbesondere sind vorstehende WLAN-Richtlinien auch für ein am Heimarbeitsplatz oder sonst extern betriebenes WLAN zu beachten, wenn von dort ein Zugang auf das Büronetzwerk eingerichtet ist.

2.13. Wir empfehlen eine strikte Trennung zwischen Büro-Anwendungen und anderen Nutzungszwecken von technischen Systemen sowie zwischen Büro-System und anderen Systemen.

2.14. Der Internetzugang darf ausschließlich über das Notarnetz hergestellt werden. Ein erhebliches Gefährdungspotential stellen alternative zusätzliche Internet-Zugänge dar, da diese Zugänge nicht durch die Sicherheitsarchitektur des Notarnetzes geschützt sind und das Notarnetz und damit auch die Zentralen Register durch Zusammenschaltung infizieren können. Aus diesem Grund sollten Systeme, die an das Notarnetz angeschlossen sind, grundsätzlich keine weiteren Internet-Anschlüsse haben.

2.15. Es dürfen keine Fernwartungs-Programme oder ähnliche Einrichtungen betrieben werden, die ständig und ohne Überwachung mit einem Server im Internet verbunden sind, um den Zugriff aus dem Internet auf das System zu ermöglichen. Sie umgehen die Sicherheitseinrichtungen des Notarnetzes und ermöglichen einen unkontrollierten Zugriff auf das System und damit auch auf die Zentralen Register.

2.16. Um einen Zugang von Unbefugten auf das System zu verhindern, dürfen alle Arbeitsplatz-PCs, Server und andere in das lokale Netzwerk eingebundene Geräte nur über eine vorherige, passwortgesicherte Anmeldung zugänglich sein. Ein solches Anmeldepasswort sollte ebenfalls kryptisch aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen bestehen sowie mindestens 10 Zeichen lang sein. Darüber hinaus sollte ein Benutzerkonto nach maximal fünf nacheinander erfolgten gescheiterten Anmeldeversuchen vorübergehend automatisch gesperrt werden.

2.17. Passwörter, PIN und Signaturkarten müssen vor dem Zugriff unberechtigter Dritter geschützt aufbewahrt werden. Passwörter und PIN zu den Zentralen Registern und zu sonstigen nur über das Notarnetz erreichbaren Diensten dürfen nicht lokal (etwa im Internet-Browser) gespeichert werden. Passwörter und PIN zu mit dem Notarnetz verbundenen Geräten dürfen nicht identisch sein mit Passwörtern und PINs, die die Nutzer an anderer Stelle verwenden. Da Administratoren über umfangreiche Berechtigungen verfügen und ihre Zugänge bei Notfällen und Servicemaßnahmen benötigt werden, sind Zugänge von Administratoren besonders sorgfältig zu sichern und zu verwalten.

2.18. Gut gesicherte Systeme sind für Angreifer schwerer zu überwinden. Deshalb ist ein Trend zu beobachten, Sicherheitslücken im organisatorischen Bereich (nachlässiger Umgang mit Benutzername und Passwort, nur schwach gesicherte Heimarbeitsplätze etc.) auszunutzen, um auf diese Weise ohne die aufwendige Überwindung von Sicherheitssystemen Zugang auf sicherheitsrelevante Bereiche zu erhalten. Zentraler Punkt eines Sicherheitskonzeptes sollte deshalb sein, über organisatorische Maßnahmen wie praxisgerechte Schulungen und Benutzerrichtlinien die Nutzung von IT in der Notarstelle sicher zu gestalten.

3. Sachgemäßer Umgang mit technischen Geräten

3.1. Die von der NotarNet GmbH zur Verfügung gestellte Notarnetzbox wird nicht Eigentum des Notars. Um Beschädigungen oder eine automatische Sperrung der Notarnetzbox zu vermeiden, sind die nachfolgenden Hinweise zur Behandlung der Geräte einzuhalten.

3.2. Die Notarnetzbox muss sorgsam behandelt werden. Sie ist vor Stößen und anderen äußeren Einflüssen zu schützen.

3.3. Die Notarnetzbox darf nur bei Umgebungstemperaturen von 0°C bis 40°C betrieben werden. Direkte Sonneneinstrahlung ist zu vermeiden.

3.4. Die relative Luftfeuchtigkeit in der Umgebung der Notarnetzbox sollte zwischen 10% und 85% (nichtkondensierend) liegen.

3.5. Links und rechts an der Notarnetzbox befinden sich Lüftungslöcher. Im Abstand von 10 cm davon dürfen sich keine Gegenstände befinden, welche die Luftzufuhr beeinträchtigen. Ein Hitzestau kann zu einem Gerätedefekt führen.

3.6. Staubansammlungen in Nähe der Notarnetzbox sind zu vermeiden. Auf den Gehäusedeckel dürfen keine Gegenstände gestellt werden.

3.7. Die Notarnetzbox ist nicht für die Montage in 19-Zoll-Schränken vorbereitet. Bitte verwenden Sie einen eigenen Gerätefachboden.

3.8. Die Notarnetzbox ist physikalisch vor unbefugtem Zugriff zu schützen, da sie funktional den Schlüssel durch die „äußere Schutzmauer“ der IT-Plattform der Bundes-notarkammer, in welcher u.a. die Zentralen Register angesiedelt sind, darstellt.

3.9. Die Notarnetzbox darf nicht geöffnet und die Sicherheitsaufkleber dürfen nicht beschädigt werden.

3.10. Ferner dürfen die Einstellungen der Notarnetzbox nicht zurückgesetzt werden.

3.11. Jeder nicht autorisierte administrative Zugriff oder Zugriffsversuch auf die Notarnetzbox führt aus Sicherheitsgründen zur Löschung aller Konfigurationsdaten, so dass eine Nutzung im Notarnetz und eine Verbindung zur IT-Plattform der Bundesnotarkammer danach nicht mehr hergestellt werden kann.

3.12. Sollten Veränderungen oder Manipulationen an der Notarnetzbox festgestellt werden oder sollte die Notarnetzbox entwendet oder beschädigt worden sein, ist umgehend die Bundesnotarkammer (notare@testamentsregister.de) oder die NotarNet GmbH (info@notarnet.de) zu informieren. Dies gilt auch bei Betriebsstörungen.

3.13. Die Notarnetzbox ist bei Beendigung des Amtes oder jederzeit auf Verlangen der NotarNet GmbH im Rahmen der vertraglichen Regelungen zurückzugeben.

3.14. Sofern die Notarnetzbox nicht durchgängig aktiviert und mit dem DSL/ISDN-Anschluss verbunden ist, ist sie zu Wartungszwecken auf Verlangen der NotarNet GmbH jederzeit, insbesondere auch außerhalb der üblichen Arbeitszeiten, in geeigneter Weise anzuschließen.

Stand: Februar 2016