Leistungen der NotarNet GmbH zur Umsetzung der „Handreichung IT-Sicherheit für Notarinnen und Notare sowie deren Beschäftigte“

STAND: 31. März 2022

Einleitung

Der Perimeterschutz stellt einen zentralen Aspekt der Sicherung des Notarbüros dar (vgl. Teil II Abschnitt 2.1 der Handreichung). Daneben weisen Bereiche wie ein ordnungsgemäßer E-Mail-Verkehr sowie eine sichere Nutzung des Internets maßgebliche Sicherheitsrelevanz auf (vgl. Teil II Abschnitt 5 und 7 der Handreichung). Hierfür stellt die NotarNet GmbH mit ihrem Angebot „NotarnetzPlus“ Lösungen bereit, die über die sichere Kommunikation der Notarbüros mit den Diensten der Bundesnotarkammer über das Notarnetz hinausgehen. Eine Beschreibung der Leistungen des NotarnetzPlus findet sich auf der Webseite der NotarNet GmbH[1] sowie im Bereich der Online-Hilfe[2].

In dieser Übersicht wird das Sicherheitsniveau der NotarnetzPlus-Leistungen vor dem Hintergrund konkreter Punkte der Handreichung betrachtet. Aus Gründen der Übersichtlichkeit orientiert sich das Schema dabei an der Kurzübersicht der Handreichung; die Priorisierung wurde unverändert übernommen.

Ergänzend findet sich in der rechten Spalte eine Bewertung der NotarNet GmbH:

⚠ steht für eine Erhöhung des Sicherheitsniveaus, die aber noch lokaler Ergänzungen bedarf

✓ steht für die Bereitstellung des benötigten Schutzes nach dem Stand der Technik

Im Vordergrund stehen dabei technische Aspekte; nicht weniger relevante organisatorische Maßnahmen sind eigenverantwortlich vom Notarbüro umzusetzen.

[1] www.notarnet.de/produkte

[2] https://onlinehilfe.bnotk.de/einrichtungen/notarnet/produkte-und-services.html

Kurzüberblick Teil I

Teil I: Allgemeine Sicherheitshinweise	
3. Sichere Konten	
Werden die nachfolgenden Hinweise zur Passwortsicherheit bei eigenen Passwörtern und denen der Beschäftigten beachtet?	⚠
Die Passwortregeln werden von den NotarnetzPlus-Produkten umgesetzt, beispielsweise bei Anlegen eines neuen WLAN-Accounts.[3] Erforderlich ist ein alphanumerisches Passwort mit einer Mindestlänge von acht Zeichen einschließlich Großbuchstaben und Sonderzeichen. Die weiteren Schutzmaßnahmen (beispielsweise Passwörter für die Anmeldung am Arbeitsplatzrechner) sind durch das Notarbüro sicherzustellen.	
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?	⚠
Alle sicherheitsrelevanten Komponenten der NotarnetzPlus-Produkte (wie beispielsweise Firewall, Endpoint-Protection, Intrusion-Detection) einschließlich der bereitgestellten Hardware werden von der NotarNet GmbH stets aktuell gehalten. Lokale Systeme im Notarbüro liegen dagegen in der Verantwortung der Amtsperson und können von der NotarNet nicht überwacht oder aktualisiert werden.	
6. Sensible Bereiche und Geräte	
Werden (organisationskritische) Geräte durch organisatorische Maßnahmen geschützt?	⚠
Zentrale sicherheitsrelevante Komponenten wie die Firewall, die zentrale Endpoint-Protection und die Intrusion-Detection sind bei der Nutzung von NotarnetzPlus im sicheren Rechenzentrum untergebracht, sodass ein unberechtigter Zugriff und eine Manipulation nicht möglich sind. Hierdurch sind die für den notariellen Alltag wichtigsten Verbindungen abgesichert. Lokale Maßnahmen werden dadurch allerdings nicht obsolet (vgl. Teil I Abschnitt 6 der Handreichung).	
8. Besonderheiten bei der Mobilarbeit	
Werden Mobiltelefone ausreichend geschützt?	✓
Die Verwendung des Angebotes „Notarnetz-Mobilzugang“ beinhaltet den überwachten Zugang zu den Diensten der Bundesnotarkammer sowie des E-Mail-Accounts. Dies sichert das Endgerät zwar nicht vollumfänglich, erhöht das Sicherheitsniveau jedoch deutlich. Ergänzende lokale Maßnahmen finden sich in Teil I Abschnitt 8.	

[3] https://onlinehilfe.bnotk.de/einrichtungen/notarnet/produkte-und-services/zubehoer/wlan-access-point.html#c2598

Kurzüberblick Teil II

Teil II: Technische Erweiterung	
2. Netzwerksicherheit	
Wird die Netzwerkintegrität durch eine Firewall geschützt?	✓
Die Nutzung von NotarnetzPlus schützt das Notarbüro nicht nur durch eine Firewall, sondern durch zusätzliche Scanning- und Monitoring-Maßnahmen, die unter anderem unbefugtes Eindringen erkennen.	
Werden deren Konfiguration und Regelwerk dokumentiert und regelmäßig überprüft?	✓
Alle NotarnetzPlus-Produkte werden im abgesicherten Rechenzentrum stets aktuell gehalten. Das Vorgehen wird vollständig dokumentiert.	
Werden wesentliche Netzwerkbereiche segmentiert?	✓
Die Nutzung von NotarnetzPlus bietet eine standardisierte Lösung für die üblichen Anwendungsfälle des Notarbüros. Die Voreinstellungen der Notarnetzbox separieren zwischen dem internen und dem externen Netz. Daneben besteht die Möglichkeit, diese Netzwerksegmentierung spezifisch zu erweitern, sofern dies ausnahmsweise erforderlich sein sollte.	
Werden die Besonderheiten beim Einsatz von WLAN beachtet?	✓
Die Nutzung von NotarnetzPlus bietet ein Produkt zum sicheren Einsatz von WLAN. Das WLAN wird nach dem Stand der Technik verschlüsselt. Für Gästezugänge und private Nutzung wird gemäß NotarnetzPlus-Konzept ein eigenes Gäste-WLAN vom Systemhaus angeboten, das im Netz-Segment für „sonstige Anwendungen“ getrennt eingerichtet wird. Die Beschränkung der Reichweite und Nutzbarkeit auf die nötigen Räume, Geräte und Beschäftigten ist durch gezielten Einsatz der WLAN-Zugänge im Notarbüro sicherzustellen.	
3. Aktualisierung von Systemen	
Werden Sicherheitsupdates unverzüglich eingespielt?	⚠
Alle sicherheitsrelevanten Komponenten der NotarnetzPlus-Produkte im zentralen Rechenzentrum wie Firewall, Endpoint-Protection und Intrusion-Detection werden stets aktuell gehalten. Lokale Systeme im Notarbüro müssen darüber hinaus durch das verantwortliche Systemhaus aktualisiert werden.	

4. Datensicherung und -wiederherstellung	
Existiert ein klares und strukturiertes Backup-Konzept?	⚠
Bei Nutzung des NotarnetzPlus-Produkts „E-Mail und mehr“ werden die Mails täglich gesichert. Dies ist kein Backup Konzept im Sinne des Teil II Abschnitt 4, beugt aber einem Datenverlust im laufenden Betrieb vor.	
5. E-Mail-Sicherheit	
Werden eingehende E-Mails bereits durch eine Software überprüft?	✓
Bei Nutzung des NotarnetzPlus-Produkts „E-Mail und mehr“ werden die Mails mehrfach überprüft. Nichtsdestotrotz ist auch das Gefahrenbewusstsein der Beschäftigten weiter relevant (vgl. Teil I Abschnitt 1 und 2).	
Werden gefährliche (z. B. ausführbare) Dateianhänge automatisch blockiert?	✓
Bei Nutzung des NotarnetzPlus-Produkts „E-Mail und mehr“ werden unverschlüsselte E-Mails, deren Inhalt oder Anhänge mit Schadcode behaftet sind, nicht zugestellt. Der Nutzer wird hierüber jedoch entsprechend informiert: Dem System bereits bekannte Viren werden automatisch blockiert; in diesem Fall erhält die Notarin bzw. der Notar per E-Mail einen Hinweis über die aussortierte Nachricht. Handelt es sich lediglich um potentiell gefährliche Inhalte oder Anhänge, erhält die Notarin bzw. der Notar ebenfalls eine Benachrichtigung per E-Mail, jedoch mit der potentiell gefährlichen E-Mail im Anhang. Die abschließende Beurteilung obliegt insoweit der Notarin bzw. dem Notar.	
12. Remote Zugriff	
Existieren klare Regeln und Maßnahmen zur Durchführung von Fernwartungen (z. B. Verschlüsselung der Fernwartungsverbindung, Protokollierung der Verbindung)?	⚠
Die Fernwartung durch die NotarNet GmbH oder von ihr beauftragter Dienstleister wird nach klaren Regeln unter Berücksichtigung strenger technischer und organisatorischer Maßnahmen durchgeführt, vgl. § 7 Absatz 3 der Nutzungsbedingungen für die Teilnahme am Notarnetz.[4]	

[4] Abrufbar unter https://notarnet.de/fileadmin/user_upload_notarnet/downloads/Nutzungsbedingungen_Notarnetz-BNotK.pdf.