IT-SICHERHEIT UND DATENSCHUTZ (TEIL 2)

Der TOM-Faktencheck zu Server, Drucker, Passwörtern und Co. im Notariat und in der Kanzlei

von RAin Heike Mareck, Dortmund

| Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, also Deutschlands höchster Hüter des Datenschutzes, genehmigte im Jahr 2022 Verhaltensregeln für Notare zu technischen und organisatorischen Maßnahmen (TOM) bei elektronischen Aufzeichnungen und Hilfsmitteln. Diese Maßnahmen sind auch für Kanzleiinhaber empfehlenswert, denn sie können vor unberechtigten Angriffen von innen und außen schützen. Prüfen Sie anhand der folgenden TOM-Checkliste, wo eventuell bei Ihnen noch Optimierungsbedarf besteht (iww.de/ak, Abruf-Nr. 49306779)! |

DOWNLOAD
TOM-Checkliste
Abruf-Nr. 49306779

Checkliste: Verhaltensregeln zu TOMS in Notariaten und Kanzleien

Fragenkatalog durchgehen	erledigt
Notebooks, Tablets und externe Speichermedien ■ Verschlüsselung nach dem Stand der Technik beachten. ■ Bei Nichtgebrauch Geräte so aufbewahren, dass sie vor Gelegenheitsdiebstahl geschützt sind (z. B. in einem abschließbaren Schrank).	
Arbeitsplatzrechner ■ Für eine Verschlüsselung nach dem Stand der Technik sorgen. ■ So aufstellen, dass sie vor unbeaufsichtigtem Zugriff oder Manipulation geschützt sind (z. B. durch Platzierung an nicht öffentlich zugänglichen Bereichen oder durch Sicht von Mitarbeitenden). ■ Wenn die örtlichen Gegebenheiten Obengenanntes nicht zulassen, muss der Druckauftrag z. B. durch eine PIN-Eingabe, einen Transponder oder eine Benutzerkarte gestartet und überwacht werden. ■ Alle Arbeitsplatzrechner und Server sowie sonstigen zentralen Komponenten, die dem Datenaustausch dienen, müssen über ein Virenschutzprogramm verfügen. Dieses muss stets aktuell gehalten werden und so konfiguriert werden, dass es Datenträger und Netze (Notarnetz, Intranet, Internet) sowie Dateien von Dritten, z. B. E-Mail-Anhänge, vor dem Öffnen prüft bzw. überwacht.	
Server ■ Der Raum, in dem sich der Server befindet, sollte für den Publikumsverkehr geschlossen sein. Ansonsten muss sichergestellt werden, dass kein unbeaufsichtigter Zugriff erfolgt. ■ Wichtige IT-Komponenten (Server, Sicherungsmedien, Register- bzw. Notarnetzbox etc.) dürfen keinen wesentlichen Umgebungsrisiken (wie extreme Luftfeuchtigkeit, Staubbelastung, Temperatur etc.) ausgesetzt sein und müssen an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz angeschlossen sein.	
Drucker ■ Verschlüsselung nach dem Stand der Technik beachten. ■ So aufstellen, dass die Drucker vor unbeaufsichtigtem Zugriff oder Manipulation geschützt sind (z. B. durch Platzierung an nicht öffentlich zugänglichen Bereichen oder nicht einsehbar). ■ Sofern die örtlichen Gegebenheiten dies nicht zulassen, muss der Druckauftrag z. B. durch eine PIN-Eingabe, einen Transponder oder eine Benutzerkarte gestartet und überwacht werden.	
Anmeldung zum Arbeitsplatzrechner, zur Notarsoftware, zur Einsicht in das Grundbuch, ZVR usw.: ■ Für unterschiedliche Zugänge unterschiedliche Passwörter verwenden. ■ Geeignete Passwortmanager einsetzen, die Passwörter nach dem Stand der Technik schützen, sowie eine Zwei-Faktor-Authentifizierung bei Nutzung von Online-Diensten sind empfehlenswert.	

Bildschirmrechner ■ Gegenüber Dritten muss sichergestellt sein, dass beim Verlassen des Raums kein unbefugter Zugriff auf den Bildschirmrechner erfolgt. ■ Nach einer angemessenen Wartezeit muss eine automatische Bildschirmsperre erfolgen. Notfalls soll die Bildschirmsperre auch bei kürzerer Abwesenheit manuell aktiviert werden können. ■ Der Bildschirminhalt muss vor neugierigen Blicken geschützt werden (z. B. durch eine entsprechende Bildschirmausrichtung oder durch den Einsatz von Blickschutzfolien). Dies gilt insbesondere für die Bildschirme im Empfangsbereich oder für den Laptop, der unterwegs – z. B. im Zug – genutzt wird.	
Öffentlich zugängliche Bereiche, z. B. Wartebereich, Flur, Empfang Ist in diesen Bereichen eine Netzwerk-Infrastruktur vorhanden, soll eine geeignete Authentifizierung nach dem Stand der Technik erfolgen. Ist dies nicht machbar, soll sich keine Netzwerk-Infrastruktur im Wartebereich befinden. Sofern ein Wireless-Local-Area-Network (WLAN) eingerichtet ist, soll sich ferner der Router oder WLAN Access Point nicht in den öffentlich zugänglichen Bereichen befinden. Sofern dies nicht anders möglich ist, dürfen die Zugangsdaten zum Netzwerk nicht auf dem Gerät stehen. Ein Einsatz der WPS-Funktion (Wi-Fi Protected Setup) soll nach dem derzeitigen Stand der Technik nicht erfolgen; der Einsatz darf nicht erfolgen, wenn sich das Gerät in einem öffentlich zugänglichen Bereich befindet.	
Passwörter ■ Passwörter dürfen nicht weitergegeben werden. ■ Es muss auf eine hinreichende Passwortsicherheit durch an aktuellen Standards orientierten Passwortrichtlinien geachtet werden. ■ Passwörter müssen unverzüglich geändert werden, wenn der Verdacht besteht, dass jemand unbefugt Kenntnis erlangt hat. ■ Darüber hinaus müssen vom Anbieter voreingestellte Passwörter (also die automatisch vergebenen Passwörter bei einer Erstanmeldung) für Software und Hardware geändert werden. ■ Nach dem Ausscheiden von Mitarbeitenden müssen die diesen individuell zugewiesenen Accounts unverzüglich deaktiviert werden. ■ Passwörter müssen an einem sicheren Ort (z. B. in einem Tresor, abschließbaren Schrank oder Passwortmanager) hinterlegt werden. ■ Das Passwort darf nicht in unmittelbarer Nähe des Arbeitsplatzrechners (z. B. unter der Tastatur oder in der Schreibtischschublade) notiert sein. ■ Passwörter sollen nicht automatisch gespeichert werden. Auch im Browser sollen keine Passwörter gespeichert sein, es sei denn, diese werden durch ein Masterpasswort zusätzlich abgesichert. ■ Sofern die betreffende Anwendung eine dahingehende Konfiguration erlaubt, sollen häufige fehlgeschlagene Anmeldeversuche zu zeitlichen Sperrungen führen.	
WLAN Für eine Verschlüsselung nach dem Stand der Technik sorgen.	
Website Muss mindestens über eine Transportverschlüsselung nach dem Stand der Technik verfügen.	
Dienstleister Dienstleister dürfen in den Arbeitsräumen nur unter angemessenen Aufsichtsmaßnahmen Arbeiten an IT-Systemen oder Telekommunikationsanlagen vornehmen.	
Administratorenrechte ■ Administratorrechte dürfen nur ausgewählten Mitarbeitern zugewiesen werden. ■ Anmeldung mit Administratorrechten soll nur während Softwareinstallationen oder Konfigurationsänderungen am System erfolgen.	
Entsorgung von Datenträger Vor der Entsorgung müssen alle Daten sorgfältig gelöscht sein, z. B. durch mehrfaches Überschreiben oder physische Zerstörung des Datenträgers.	

Gäste-WLAN Ist ein Gäste-WLAN in den Kanzleiräumen vorhanden, müssen mindestens solche Geräte, die keinen Serverzugriff erfordern, ein eigenes Netzwerksegment bilden (z. B. mit dem Internet verbundene Alarmanlagen, Frankiermaschinen, Kartenzahlungsgeräte).	
Gesamtes Netzwerk ■ Das gesamte Netzwerk muss durch eine Firewall geschützt werden. ■ Innerhalb des Netzwerks gilt: Für eine geeignete Netzwerksegmentierung sorgen, z. B. mittels Virtual Local Area Network (VLAN). ■ Eingegangene E-Mails müssen bereits mittels technischer Vorkehrungen auf Spam und Schadsoftware untersucht werden.	
Netzwerk-Ports Nicht benötigte Netzwerk-Ports müssen deaktiviert werden.	
Private Mitarbeitergeräte Private Mitarbeitergeräte dürfen nicht für die Verarbeitung von personenbezogenen Daten von Mandaten verwendet werden.	
Externe Quellen ■ Aus externen Quellen bezogene Dokumente müssen vor dem Öffnen auf Schadsoftware überprüft werden. ■ In Office-Anwendungen sollten nur überprüfte und digital signierte Makros aktiviert werden, sofern dies technisch möglich ist, und insbesondere weitere Systeme und Software (wie die eingesetzte Notarsoftware) ohne Einschränkungen verwendet werden können.	
Fernwartung Technische und/oder organisatorische Vorkehrungen gegen Missbrauch treffen, wie z. B.: ■ Protokolle: Welche Veränderungen wurden vorgenommen und auf welche Daten wurde zugegriffen? ■ Notieren, wann der Beginn der Fernwartung und durch wen ausgelöst wurde. ■ Sicherstellen, dass der Notar bzw. die Mitarbeiter die Fernwartung mitverfolgen und jederzeit abbrechen können. ■ Zugriffsrechte des Technikers auf ein Minimum beschränken. ■ Fernwartungsdaten verschlüsselt und über eine geschützte Verbindung übertragen.	

Notfall- und Backup-Konzept
■ In der Kanzlei/dem Notariat muss ein Notfallkonzept für Zwischenfälle vorliegen. Hier muss geregelt sein, wer bei einem Zwischenfall damit beauftragt wird, wiederherstellende Maßnahmen einzuleiten. Sofern dies ein externer IT-Dienstleister ist, sollen auch die Mitarbeiter ihren Ansprechpartner und die Kontaktdaten kennen.
■ Der Notar/der Kanzleiinhaber muss ein Backup-Konzept erstellen und umsetzen lassen. Dieses soll sich an folgenden Maßstäben orientieren:
  ■ Zuständigkeit für das Backup bestimmen, samt Stellvertretung bei Urlaub, Krankheit etc.
  ■ Das Backup umfasst sämtliche Daten.
  ■ Das Backup folgt der sog. 3-2-1-Regel, d. h. es erfolgen drei Datenspeicherungen auf mindestens zwei verschiedenen Backupmedien (auch „Offline"), wobei sich ein Backup-medium an einem externen, hinreichend abgesicherten Standort befindet (z. B. Tresor, anderer Brandabschnitt). So schützt man die Daten vor Einbrüchen, Brand, Wasserschäden und ähnlichen Gefahren. Das Backup wird regelmäßig auf Vollständigkeit, Korrektheit und Wiederherstellbarkeit geprüft.
  ■ Backupmedien und der Datenübertragungsweg sind verschlüsselt.
  ■ Empfehlenswert ist ferner eine Einschränkung der Schreibrechte auf dem Backupsystem.	

Kontrollen ■ Einhaltung der genannten Verhaltensregeln muss turnusmäßig überprüft werden. ■ Durch physischen Rundgang durch die Räume sollen sämtliche Elemente überprüft werden. ■ Für einen besseren Überblick: Netzwerkplan und Dokumentation der IT-Infrastruktur der Kanzleiräume erstellen.	

Mitarbeiter ■ Mitarbeiter dürfen nur die zur Erledigung ihrer Aufgaben notwendigen Berechtigungen erhalten. Tipp: Erstellen Sie ein Rechte- und Rollenkonzept. ■ Überprüfen Sie die vergebenen Rechte regelmäßig auf ihre Aktualität bezüglich der jeweiligen Tätigkeitsfelder. ■ Mitarbeiter müssen im erforderlichen Umfang zu Fragen der IT-Sicherheit und der Sicherheit der Verarbeitung personenbezogener Daten qualifiziert und regelmäßig sensibilisiert werden. Insbesondere muss der Notar/der Kanzleiinhaber die Mitarbeiter für die Gefahren externer Inhalte, etwa beim unbedachten Öffnen verdächtiger E-Mail-Anhänge und Links, beim Download von Dateien aus dem Internet und bei der Nutzung fremder Speichermedien (z. B. des USB-Sticks eines Dritten) sensibilisieren. ■ Im Zweifel müssen sichernde Maßnahmen ergriffen werden, z. B. eine Nachfrage beim Absender der E-Mail, eine Überprüfung des USB-Sticks vor der Nutzung oder dessen alleinige Verwendung an einem speziell gesicherten Arbeitsplatzrechner. ■ Daten sollen nicht lokal auf dem Arbeitsplatzrechner gespeichert werden, sondern auf Servern und Festplatten, die dem Backup unterliegen. Der Notar muss die Mitarbeiter auf die Gefahr des unwiederbringlichen Verlusts lokal gespeicherter Daten hinweisen.	
Notar/Kanzleiinhaber/anderer Verantwortlicher ■ Sofern von außerhalb auf das interne Netzwerk zugegriffen wird (z. B. bei einer Auswärtsbesprechung oder -beurkundung oder bei Heimarbeit), muss dies über eine sichere VPN-Verbindung erfolgen. Dies gilt nicht für den Fall einer Fernwartung. ■ Der Verantwortliche soll besonders wichtige Systemelemente mehrfach vorhalten. ■ Zusammen mit einer IT-Fachkraft soll der Notar regelmäßig prüfen, wie sich die Belastbarkeit der Systeme erhöhen lässt, z. B. durch eine Abgrenzung kritischer Komponenten, das Einfügen weiterer Redundanzen (wie eines sog. RAID-Systems) oder einen Ausbau von Speicherkapazitäten. ■ Der Verantwortliche darf in den Kanzleiräumen nur Betriebssysteme verwenden, die regelmäßige Updates bereitstellen. Sicherheits-Updates (insbesondere für das Virenschutzprogramm, aber auch für Firewall, Router, Betriebssystem, Web-Browser, Notar-/Anwaltssoftware, andere Office-Anwendungen etc.) müssen regelmäßig durchgeführt werden. Auch bestimmte Hardware-Komponenten müssen regelmäßig gewartet und aktualisiert werden, wobei hierfür eine individuelle Betrachtung möglicher Schwachstellen erforderlich ist.	

PRAXISTIPP | Noch zwei Tipps zum Server:
- Damit der Server im Sommer nicht „schlapp macht", sollten Sie für eine ausreichende Lüftung sorgen (entweder per Fenster oder Klimagerät).
- Durch den Serverraum sollten keine Wasserleitungen führen. Außerdem sollten auch keine Räume mit Wasserrohren (z. B. Küche, Toiletten) über bzw. neben dem Serverraum liegen.

Server kühl und trocken stellen

Beachten Sie | Ggf. stellt auch noch Ihr Cyber-Versicherer zusätzliche Anforderungen, die Sie beachten müssen (z. B. abgestuftes Rechtekonzept mit administrativen Kennungen für einen IT-Verantwortlichen). Und auch die dargestellten Verhaltensregeln sind nicht von heute auf morgen gemacht, das ist klar. Laut den Verhaltensregeln sollte der Kanzlei-/Notarinhaber auf drei Regelungsebenen zurückgreifen:

Regelungsebenen einführen

- Verbindliche Regelungen ohne Abweichungsmöglichkeit („muss"/„darf nicht"/"darf nur, wenn")
- Verbindliche Regelungen mit Abweichungsmöglichkeit („soll"/„soll nicht")
- Unverbindliche Empfehlungen („empfehlenswert", Beispiele)