IT-Sicherheit der EGVP-Infrastruktur

Aktualisierung 28.08.2018

Wir möchten zu Fragen, die im Kontext der Diskussion um das besondere elektronische Anwaltspostfach (beA) gestellt werden, wie folgt Stellung nehmen:

Alle im Abschlussgutachten zur IT-Sicherheit des beA genannten Schwachstellen sowie in der öffentlichen und internen Diskussion aufgeworfenen Sicherheitsfragen werden regelmäßig und kurzfristig von den zuständigen Stellen geprüft. Dabei wurde festgestellt, dass die EGVP-Infrastruktur der Justiz nicht betroffen ist. Vorschläge zur Verbesserung der Informationssicherheit, die angemessen, technisch umsetzbar und wirtschaftlich sind, werden selbstverständlich dennoch aufgegriffen und im Rahmen der regulären Weiterentwicklung der Systeme und Prozesse umgesetzt.

Hier sind die Antworten auf die am häufigsten genannten Fragen:

1. Ist die EGVP-Infrastruktur der Justiz von den im beA diskutierten Schwachstellen betroffen?

Nein. Alle bekannten Schwachstellen, die derzeit zum beA diskutiert werden, sind für die EGVP-Infrastruktur nicht einschlägig. Technologien, wie die vom beA genutzte Client Security oder HSM, werden und wurden in der Justiz nicht verwendet.

Alle EGVP-Komponenten basieren auf dem OSCI-Standard. Die OSCI-Anpassungen, die regelmäßig auch sicherheitsrelevante Änderungen umfassen, sind auf der Internetseite der Koordinierungsstelle für IT-Standards des IT-Planungsrats (KoSIT) dokumentiert (https://www.xoev.de/downloads-2316#Standards). In den EGVP-Komponenten der Justiz kommen nur aktuelle, nach Stand der Technik fehlerfreie OSCI-Bibliotheken zum Einsatz.

2. Ist der Absender von EGVP-Nachrichten eindeutig erkennbar?

Es gehört auf Grund der Gesetzeslage zu den Pflichten der Justiz, für jedermann den elektronischen Zugang zur Justiz zu gewährleisten[1]. Deshalb ist es möglich, ein EGVP-Postfach anzulegen, ohne einen Freischaltungsprozess zu durchlaufen. Angaben in EGVP-Postfächern für jedermann werden beim Anlegen des jeweiligen EGVP-Postfachs nicht geprüft.

Die Authentizität einer Person, die Nachrichten aus einem solchen nicht authentifizierten EGVP-Postfach übermittelt, ergibt sich aus der stets für die Ersetzung der Schriftform erforderlichen qualifizierten elektronischen Signatur. Die Bezeichnung des Postfachs, die grundsätzlich frei wählbar ist, dient nicht zur Authentifizierung des Absenders. Sie ist eher vergleichbar mit den Angaben auf einem Briefumschlag bei der Papierpost.

Daneben gibt es im EGVP-System authentifizierte Postfächer, bei denen auf die Herkunft einer Nachricht von einem bestimmten Absender vertraut werden kann. Der Anlage solcher Postfächer geht ein Prüfungs- und Freischaltverfahren voraus. Die Postfächer der Gerichte und Staatsanwaltschaften sowie die sogenannten besonderen Postfächer (beA, beBPo und beN) haben dieses Freischaltverfahren durchlaufen und sind im Verzeichnisdienst durch eine entsprechende Rollenangabe als sichere, authentifizierte Postfächer erkennbar. Im Übrigen können nichtauthentifizierte EGVP-Nutzer andere nichtauthentifizierte Postfächer nicht adressieren.

3. Wann werden EGVP-Postfächer gesperrt?

Jeder EGVP-Postfachinhaber kann sein Postfach jederzeit selbst über eine Funktion der Sende- und Empfangskomponente löschen. Sollte ein Nutzer nicht mehr über die Zugangsdaten zu seinem EGVP-Postfach verfügen, kann das EGVP-Postfach im Verzeichnisdienst gesperrt werden, da es andernfalls weiterhin adressierbar ist, der Inhaber die Nachrichten aber nicht mehr zur Kenntnis nehmen kann.

Für diesen Fall wird ein Sperrdienst angeboten. Nicht authentifizierte EGVP-Postfächer, für die die Sperrung erbeten wird, werden zunächst lediglich deaktiviert. Sollte irrtümlich eine Postfachsperrung veranlasst worden sein, kann dies auf Bitten des berechtigten Inhabers nach Prüfung seiner Berechtigung schnell rückgängig gemacht werden.

[1] § 130 a Abs.3, 1.Variante ZPO i.V.m. § 4 Abs. 1 Nr. 2 ERVV

4. Bewältigt die EGVP-Infrastruktur die erwartete Zahl von Nachrichten?

Die EGVP-Infrastruktur der Justiz ist darauf ausgerichtet, eine Vielzahl von Nachrichten empfangen und versenden zu können, um den Anforderungen des elektronischen Rechtsverkehrs heute und in Zukunft gerecht zu werden. Es werden regelmäßig Lasttests durchgeführt. Die übrigen Anwender des EGVP müssen ebenfalls darauf achten, dass ihre Infrastruktur bedarfsgerecht ist. Die von der Justiz eingesetzten Komponenten werden erweitert, falls Engpässe ersichtlich werden.

Das Risiko von DDoS-Attacken betrifft ausnahmslos alle Anbieter von Internetdiensten. Alle Komponenten der EGVP-Infrastruktur der Justiz werden in hochleistungsfähigen und sicheren Rechenzentren betrieben, die alle Vorkehrungen zur Abwehr etwaiger DDoS-Attacken nach dem Stand der Technik getroffen haben. Eine Stellungnahme der VITAKO kann hier zurate gezogen werden: https://www.vitako.de/Publikationen/Vitako-Pressemitteilung%20Sicherheitsdiskussion%20rund%20um%20das%20beA.pdf

5. Wird der bereits abgekündigte EGVP-Classic-Client noch gepflegt?

Der EGVP-Classic-Client ist seit geraumer Zeit abgekündigt. Die Bereitstellung von EGVP-Sende- und Empfangskomponenten wird künftig den Softwareherstellern überlassen. Die Abschaltung des EGVP-Classic-Clients war ursprünglich zum 1.1.2018 beabsichtigt. Da jedoch das beA seit Ende Dezember 2017 nicht zur Verfügung steht, wird der EGVP-Classic-Client vorübergehend weiter bereitgestellt, um den Nutzern den elektronischen Rechtsverkehr weiterhin zu ermöglichen. Im Mai 2018 hat die Bund-Länder-Kommission für Informationstechnik in der Justiz entschieden, den EGVP-Classic-Clients bereitzustellen, bis das beA wieder genutzt werden kann.

Unabhängig von der Abkündigung wird der EGVP-Classic-Client, so wie jede andere Software, jedes Betriebssystem und jede Mobiltelefon-App ständig gepflegt und aktualisiert. So wird für die Einspielung von Updates ein sogenannter Installer bereitgestellt, der sicherstellt, dass die Aktualisierungen automatisch im Hintergrund, ohne dass der Anwender tätig werden muss, erfolgen können.

6. Ist das von EGVP verwendete Verschlüsselungsverfahren sicher?

Im Abschlussgutachten zur IT-Sicherheit des beA wird unter anderem festgestellt: „Es werden unsichere Padding-Algorithmen verwendet, die Angriffe auf damit verschlüsselte Daten erlauben."

Nachrichten werden in EGVP doppelt verschlüsselt, und zwar bereits auf dem Rechner des Absenders. Das genannte Padding-Verfahren kommt nur bei der Verschlüsselung des sogenannten inneren Umschlags zur Anwendung. Für die Verschlüsselung des äußeren Umschlags wird ein sicheres Verfahren genutzt. Es ist somit nach Stand der Technik nicht möglich, die Schwachstelle in Padding-Algorithmen zu verwenden, um EGVP-Nachrichten zu entschlüsseln.

Die Justiz hat die Feststellungen im Gutachten aufgegriffen und führt für die Verschlüsselung des inneren Umschlags einer EGVP-Nachricht ebenfalls die Nutzung eines OAEP-Algorithmus ein.