IT-Sicherheit der EGVP-Infrastruktur

08.02.2018

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

1. Ist die EGVP-Infrastruktur der Justiz von der beA-Sicherheitsdiskussion 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, 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 https://www.xoev.de/downloads-2316#Standards dokumentiert. 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.

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

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 sog. 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.

4. Bewältigt die EGVP-Infrastruktur eine Vielzahl 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 ihr Netzanschluss 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 wird die Bund-Länder-Kommission für Informationstechnik in der Justiz über die Abschaltung entscheiden.

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.

Zuletzt wurde der EGVP-Installer am 01.02.2018 aktualisiert.

Durch einen vertraulichen Hinweis war es möglich, eine Schwachstelle zu identifizieren, die ausschließlich die Installationsroutine betraf. Wie für einen solchen Fall vorgesehen, wurde noch am selben Tag ein Update zur Behebung der Schwachstelle bereitgestellt. Das Computer Emergency Response Team der Bundesverwaltung – CERT-Bund – wurde informiert. Im Rahmen des Updates des EGVP-Installers wurde zudem die (gekapselte) JAVA-Version aktualisiert.