Jörn Erbguth
Legal Tech Berater
Chemin du Champ d'Anier 15
CH-1209 Genf
joern@erbguth.ch
+41 787256027

Genf, 8.2.2018

EGVP: Vorbildliches Sicherheitsmanagement aber konzeptuelle Schwachstellen

In meinem Artikel über den beAthon in der jurPC vom 30.1.2018 hatte ich darüber berichtet, dass dort auch Schwachstellen im EGVP diskutiert wurden. Da ich die „Schwachstellen" im Einzelnen nicht beschrieben hatte, diese inzwischen aber u.a. von Hanno Böck in Golem veröffentlicht bzw. behoben wurden, möchte ich dies hiermit nachreichen. Inzwischen hat auch die BLK Arbeitsgruppe „IT-Standards in der Justiz" eine Stellungnahme dazu abgegeben. Vorab schon einmal eines: Für Panik besteht keine Veranlassung. Das EGVP kann uneingeschränkt weiter genutzt werden.

Eine konzeptionelle Schwachstelle beim EGVP betrifft das nicht validierte Anlegen von Postfächern und das nicht validierte Löschen bzw. Deaktivieren derselben. Bürgerpostfächer können ohne jegliche Überprüfung unter beliebigen Namen angelegt werden. Zudem kann man sich ein Softwarezertifikat dazu ausstellen lassen – auch ohne Überprüfung. Aus Sicht des EGVP ist das ein bürgerfreundliches Feature – es ermöglicht jedoch SPAM, Phishing-Nachrichten oder das Verteilen von Malware unter falschem Namen. Diese Probleme kennen wir nur zu gut von e-Mail – einem ebenso offenen System. In der Praxis stellt diese Art des Missbrauchs beim EGVP allerdings noch kein Problem dar. Trotzdem wäre es aus meiner Sicht geboten, hier zusätzliche Sicherheitshürden einzubauen. Eine Verifizierung der bei der Postfacheröffnung angegebenen e-Mail-Adresse und ggf. auch der Handynummer über Bestätigungscodes ist inzwischen bei fast allen Internetdiensten Standard und hält die Hürden für die Nutzung trotzdem niedrig. Im beA-Client sollten zudem nicht-authentifizierte Nachrichten von anonym eröffneten Bürgerpostfächern als solche hervorgehoben werden, damit Anwälte beim Öffnen dieser Nachrichten besondere Vorsicht walten lassen.

Beim OSCI-Protokoll, welches dem EGVP zu Grunde liegt, gab es Mitte 2017 eine Schwachstelle, die einen Denial of Service Angriff (DOS) möglich machte. Dabei kann das System durch eine Überlastung mit künstlich generierten Anfragen so blockiert werden, dass es für echte Anfragen nicht mehr zur Verfügung steht. Inzwischen wurde diese Schwachstelle entschärft. Kommen die Anfragen von der gleichen IP-Adresse, werden diese geblockt. Was weiterhin möglich ist, ist ein Distributed Denial of Service Angriff (DDOS). Dabei werden die Anfragen von verschiedenen IP-Adressen getätigt. Dies ist möglich, in dem z.B. eine Serverfarm dafür angemietet wird, TOR mit wechselnden Endknoten oder ein illegales Botnet verwendet wird. Vollständig absichern gegen ein DDOS-Angriff lässt sich ein System nicht. Beim beAthon wurde jedoch die Meinung vertreten, dass hier noch mehr getan werden sollte.

Ein dritter, positiv gelöster Punkt betrifft den Support für den EGVP-Clients. Ein sicherheitskritisches System ohne Support einzusetzen, ist fahrlässig. Umso mehr irritierte die Nachricht am 25. Januar im EGVP-Newsletter, dass für den EGVP-Client kein Support mehr geleistet würde. Es wird nun aber nicht nur Support geleistet, sondern das Sicherheitsmanagement ist vorbildlich. Nachdem von jurmatix Legal Intelligence ein Sicherheitsproblem gemeldet wurde, wurde kurz danach am 1.Feburar für den EGVP-Client eine neue Version mit einem entsprechenden Sicherheitsupdate bereitgestellt.

Gravierende Sicherheitslücken treten leider in fast allen IT-Systemen auf. Zuletzt hielten uns Meltdown und Spectre in Atem, die praktisch alle Rechner unsicher gemacht haben. Entscheidend ist dabei, dass professionell auf diese Sicherheitslücken reagiert wird. Selbst große Firmen wie z.B. Intel passiert es da, dass sie durch beschönigende Kommunikation, fehlerhafte Patches oder unprofessionelles Sicherheitsmanagement den entstandenen Schaden unnötig vergrößern. Gerade deshalb versucht der Gesetzgeber durch Vorschriften wie z.B. Art. 5 Abs. 1 Bst. f i.V.m. Abs. 2 DS-GVO oder dem IT-Sicherheitsgesetz für eine Verbesserung des Sicherheitsmanagements zu sorgen. Konterkariert werden diese Bestrebungen allerdings dadurch, dass staatliche Stellen Sicherheitslücken zum Eindringen in fremde Systeme erwerben.