BUNDESRECHTSANWALTSKAMMER

Der Vizepräsident

Bundesrechtsanwaltskammer
Littenstraße 9 | 10179 Berlin

An die
Präsidentinnen und Präsidenten
der Rechtsanwaltskammern

BRAK-Nr. 039/2018
Az. beA-ERV

Berlin, 30.01.2018

vorab per E-Mail

beAthon am 26. Januar 2018

Anlagen:
1. Atos Stellungnahme zum beA v. 26.01.2018
2. Deinstallationsanleitung der beA Client Security für Windows
3. Deinstallationsanleitung der beA Client Security für MAC-Systeme

Sehr geehrte Präsidentinnen und Präsidenten,
sehr geehrte Damen und Herren Kolleginnen und Kollegen,

am vergangenen Freitag fand der sogenannte beAthon in Berlin statt. Im Anschluss daran hatten wir zunächst ad hoc von einem bei dieser Veranstaltung diskutierten, möglichen Sicherheitsrisiko berichtet. Hier folgt nun ein ausführlicher Bericht über den beAthon.

Ziel des beAthon war es, mit unabhängigen Experten und Journalisten ins Gespräch zu kommen, um die Behebung aktueller Schwachstellen im technischen System des beA konstruktiv zu diskutieren. Teilnehmer des beAthon waren neben der BRAK deshalb auch vorrangig IT-Experten, zum Beispiel Herr Drenger und zwei weitere Mitglieder des Chaos Computer Clubs (CCC), Vertreter der secunet Security Networks AG, die von der BRAK beauftragt ist, ein technisches Gutachten zur Sicherheit des beA zu erstellen, sowie Vertreter des EDV-Gerichtstags e. V., des DAV, des BMJV und zwei Fachjournalisten. Rechtsanwalt Professor Dr. Ory, Vorsitzender des EDV-Gerichtstags e.V., moderierte die Veranstaltung.

Atos hatte eine Teilnahme leider einige Tage zuvor abgesagt, obwohl es ursprünglich eine mündliche Zusage gab. Atos gab wenige Stunden vor dem beAthon gegenüber der Presse eine Stellungnahme ab, die als Anlage beigefügt ist. Darin erläuterte Atos die der BRAK zur Verfügung gestellte beA-Software in der neuen Version 2.0.9. Demnach wird die neue beA Client Security bei der Installation auf den Rechner der Nutzer ein individuelles, lokales Zertifikat erstellen. Dieses Zertifikat soll die sichere Verbindung zwischen beA Client Security und beA-Webanwendung ermöglichen und nur mit

eingeschränkten Rechten ausgestattet sein. Hintergrund dieser Aktualisierung sind vor Weihnachten durch den Chaos Computer Club gemeldete Sicherheitsrisiken, die auf Schwachpunkte in eben dieser Verbindung fokussieren. Die beA Client Security ist ein zentrales Programm der beA-Anwendung, das die Anwältinnen und Anwälte zur Nutzung des elektronischen Anwaltspostfachs auf ihrem jeweiligen PC installieren.

Die anwesenden Experten waren sich einig, dass die von Atos vorgeschlagene Lösung zur Behebung dieses Problems prinzipiell geeignet ist. Nun komme es darauf an, die Lösung auch operativ fehlerfrei umzusetzen. Die BRAK hat secunet deshalb damit beauftragt, die durch Atos umgesetzte Lösung zu begutachten.

Fazit: Wenn die nun skizzierte Lösung einer veränderten beA Client Security gut umgesetzt wird und die von der BRAK eingesetzten Gutachter sie als angemessen sicher bewerten, können wir beA unverzüglich wieder zur Verfügung stellen.

Ein wesentliches Ergebnis des beAthon war überdies die klare Aussage der großen Mehrheit der anwesenden IT-Experten (darunter alle Vertreter des Chaos Computer Clubs), dass sie es grundsätzlich für möglich erachten, die hohen Sicherheitsanforderung an das System innerhalb der bestehenden Konstruktion umzusetzen. Dabei erkennen sie an, dass die Nutzung eines sogenannten Hardware Security Moduls (HSM) Industriestandard darstellt und ein hohes Sicherheitsniveau gewährleistet, sofern es auch entsprechende Verhaltensregeln für den Betreiber der Infrastruktur des beA-Systems gibt. Das beA-HSM ist eine spezielle Hardware-Komponente des beA-Systems. Hier findet die kryptografische Umschlüsselung des Schlüsselmaterials statt, mit dem die im beA versendeten Nachrichten verschlüsselt sind. Diese Umschlüsselung gewährleistet, dass es verschiedene Zugangsberechtigungen für den Nachrichtenabruf gibt, so wie es der Gesetzgeber vorgeschrieben hat. Dazu erörterten die Teilnehmer auch die Frage, inwieweit das derzeitige System aufgrund der Umschlüsselung terminologisch als ein Ende-zu-Ende verschlüsseltes System bezeichnet werden könne.

In der unter den teilnehmenden Experten kontroversen Diskussion über weitere Schritte nach einer Wiederinbetriebnahme des beA erörterten die Teilnehmer die technischen und rechtlichen Rahmenbedingungen des beA-Systems als Kommunikationsplattform zur Justiz und die damit für das beA-System einhergehenden Vorgaben. Diese Diskussion drehte sich insbesondere um den Punkt, wie mittels neuester Krypto-Technologien unter Verzicht auf die HSM eine Verschlüsselung unter Wahrung der gesetzlichen Vorgaben möglich ist. Es herrschte aber weitgehend Einigkeit, dass Modifikationen an der Sicherheitsarchitektur, respektive bei der Frage Umschlüsselung in den HSM oder nicht, bei der Fortentwicklung des beA und der justizseitigen Systeme berücksichtigt werden sollten. Die Teilnehmer diskutierten unter dem Stichwort einer Weiterentwicklung des beA weitere technische Einzelheiten. Dabei ging es unter anderem um die Wahrscheinlichkeit der Ausnutzung von Cross-Site-Scripting-Lücken und um die Anbindung des beA an das Elektronische Gerichts- und Verwaltungspostfach (EGVP).

Der Chaos Computer Club wies im Verlauf des beAthon auf eine in seinen Augen wesentliche Sicherheitsproblematik hin. Herr Drenger bemängelte nochmals die Nutzung veralteter Software-Bibliotheken bei der Programmierung der beA Client Security. Atos hatte bereits mitgeteilt, dass in der neuen, aktualisierten Version des beA der Zugriff auf aktuelle Software-Bibliotheken sichergestellt sei, nachdem Herr Drenger diesen Sachverhalt bereits am 20. Dezember gemeldet hatte.

Auf dem beAthon führte der Chaos Computer Club nun erstmals aus, weshalb er diesen Sachverhalt für so wichtig erachtet: Denn durch die Verwendung veralteter Software-Bibliotheken sei die beA Client Security ihrer Ansicht nach von einer sogenannten Java-Deserialisierungslücke betroffen. Das bedeutet, dass – sollte der beA-Nutzer mit seinem Rechner infizierte Webseiten besuchen und zuvor auf den Startknopf der alten, auf dem Rechner noch vorhandenen beA Client Security gedrückt haben – Unberechtigte die Java-Deserialisierungslücke nutzen könnten, um Programmcodes auszuführen. Ein Angreifer könne also im äußersten Fall Software auf dem Rechner des Anwalts starten. Die anwesenden Experten waren gemeinschaftlich der Auffassung, dass diese Java-Deserialisierungslücke auch dann auftritt, wenn, wie es aktuell der Fall ist, das beA gar nicht in Betrieb ist. Es genüge, so der CCC, dass sich die alte beA Client Security auf dem Rechner des Anwalts oder der Anwältin im Autostart des Rechners befinde und dann nicht korrekt abgebrochen werde, sondern im Hintergrund aktiv bleibe. Atos hatte bisher immer die Auffassung vertreten, dass ältere Java-Bibliotheken kein Sicherheitsrisiko darstellen.

Nachdem Atos sich kurzfristig auf Nachfrage während des beAthon nicht abschließend zu den Hinweisen des CCC äußerte, hat sich die BRAK dazu entschlossen, höchst fürsorglich alle Rechtsanwältinnen und Rechtsanwälte unverzüglich über die Einschätzung der Experten des beAthon zu informieren und sie dazu aufzufordern, die beA Client Security im Autostart zu deaktivieren. Eine Anleitung zur Deaktivierung bzw. zur Deinstallation der beA Client Security für Windows- und MAC-Systeme erhalten Sie anbei.

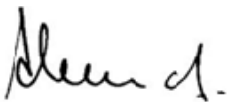
Schließlich diskutierten die Teilnehmer des beAthon auch über die Veröffentlichung des Quellcodes der Client Security. Es gibt Initiativen, die die Veröffentlichung des Quellcodes fordern. Die BRAK hat in der Diskussion klargestellt, dass ihr die Freigabe des Quellcodes aufgrund der Verwendung von Programmcodes von Dritten im Moment nicht möglich ist. Die BRAK hat sich mit dieser Frage bereits in der Vergangenheit beschäftigt und wird sie bei der Weiterentwicklung des beA auch unter Berücksichtigung der Anforderungen der Justiz für die Zukunft erneut prüfen.

Der beAthon hat weitere, gute Erkenntnisse gebracht, welche die BRAK als Anregungen für die Fortentwicklung des beA nutzen wird. Daher ist sie auch an einem weiteren Dialog mit den Netzexperten interessiert.

Der nächste Schritt zur raschen Wiederinbetriebnahme des beA-Systems ist nun die Erstellung des Gutachtens durch die secunet AG. Sollte das Gutachten ein angemessen hohes Sicherheitsniveau attestieren, wird die BRAK der Präsidentenkonferenz vorschlagen, das beA dann unverzüglich wieder in Betrieb zu nehmen. Die BRAK beabsichtigt, das Gutachten danach zu veröffentlichen.

Wir halten Sie unterrichtet.

Mit freundlichen kollegialen Grüßen



Dr. Martin Abend

From: Atos Presse [mailto:Atos@h-b-a.de]
Sent: Friday, January 26, 2018 10:00 AM
Subject: Stellungnahme zum besonderen elektronischen Anwaltspostfach (beA)

Stellungnahme zum besonderen elektronischen Anwaltspostfach (beA)

München, 26. Januar 2018 - Atos, ein führender Anbieter für die digitale Transformation, ist von der Bundesrechtsanwaltskammer (BRAK) mit der Entwicklung, der Implementierung und dem Betrieb des "besonderen elektronischen Anwaltspostfachs (beA)" beauftragt worden. Die Lösung besteht aus einer zentralen Anwendung, die sich in deutschen Atos-Rechenzentren befindet, einer Browserbasierten Web-Anwendung und einer lokal installierten Client-Anwendung. Darüber hinaus gibt es Schnittstellen zu den entsprechenden Systemen der Justiz, der Rechtsanwaltskammern sowie Kanzleisoftware-Anwendungen. Der Vertragsbeginn war Oktober 2014. Seit Projektbeginn Ende 2014 wurden in mehreren Zwischenschritten Entwicklungsstufen der Lösung eingeführt und Elemente weiterentwickelt. Die Umsetzung des beA erfolgte gemäß konzeptioneller Vorgabe der BRAK und berücksichtigte jeweils gültige gesetzliche Vorgaben. Am 28. November 2016 hat die BRAK als Auftraggeber die Lösung den Rechtsanwälten zur Verfügung gestellt.

Am 21. Dezember 2017 wurde durch externe IT-Experten eine Sicherheitslücke bei der sicheren Kommunikation zwischen Browser und Client-Anwendung festgestellt. Ein Zertifikat war zusammen mit dem zugehörigen privaten Schlüssel Bestandteil der installierten Client-Anwendung und wurde damit öffentlich gemacht. Hierdurch war die Sicherheit des Zertifikates nicht mehr gewährleistet und es wurde durch den Anbieter gesperrt. Es handelte sich allein um ein Problem in der Kommunikation des lokalen Browsers mit der Client-Anwendung auf dem Client des Anwalts - die Sicherheit der zentralen Anwendung in den Rechenzentren sowie der Schnittstelle zu den Kanzleisoftware-Anwendungen war hiervon nicht betroffen. Die sichere Kommunikation zwischen den beA-Postfächern war zu jedem Zeitpunkt gewährleistet.

Um sicherzustellen, dass das beA schnellstmöglich wieder verfügbar ist, hat Atos kurzfristig ein neues Zertifikat zur Verfügung gestellt. Am 22. Dezember 2017 hat Atos allerdings festgestellt, dass dieses neue Zertifikat mit zu weitreichenden Rechten ausgestattet war. Angreifer wären mit diesem Zertifikat in der Lage gewesen, Identitäten zu fälschen (Man-in-the-middle Attacken). Atos informierte den Kunden BRAK umgehend. Am gleichen Tag hat die BRAK das beA offline genommen.

Mittlerweile hat Atos dem Kunden BRAK eine neue Version der beA Client-Anwendung zur Verfügung gestellt. Diese Version ist wie folgt überarbeitet:

Die Client-Anwendung erstellt bei der Installation ein individuelles, lokales Zertifikat auf dem Rechner des Anwalts, welches die sichere Kommunikation zwischen Client-Anwendung und Browser ermöglicht. Dieses Zertifikat ist nur in der lokalen Installation bekannt und mit eingeschränkten Rechten ausgestattet. Hierdurch wird der Schutz gegen den missbräuchlichen Einsatz des Zertifikats massiv erhöht. Die Funktionstüchtigkeit und die Sicherheit der Lösung soll durch ein von Atos beauftragtes externes Security-Gutachten bestätigt werden.

Aus Sicht von Atos war mit der Bereitstellung der neuen Lösung die potenzielle Sicherheitslücke in der beA Browser-Anwendung geschlossen. Die Entscheidung über die erneute Inbetriebnahme des Systems liegt bei der BRAK. Die Rechte an dem Quellcode liegen ebenfalls bei der BRAK beziehungsweise bei den Herstellern der

genutzten Standardsoftware-Komponenten.
Die identifizierten Sicherheitsprobleme betrafen ausschließlich die lokale Kommunikation zwischen dem Browser und der Client-Anwendung - weder die zentralen Anwendungen noch die Schnittstelle zu Fachanwendungen waren hiervon direkt betroffen.

Die Sicherheit und Integrität sind wiederhergestellt und das System ist in der aktuell vorliegenden Ausbaustufe voll einsatzfähig.

Über Atos
Atos ist ein weltweit führender Anbieter für die digitale Transformation mit circa 100.000 Mitarbeitern in 72 Ländern und einem Jahresumsatz von rund 12 Milliarden Euro. Als europäischer Marktführer für Big Data, Cybersecurity, High Performance Computing und Digital Workplace unterstützt Atos Unternehmen mit Cloud Services, Infrastruktur- und Datenmanagement sowie Business- und Plattform-Lösungen. Hinzu kommen Services der Tochtergesellschaft Worldline, dem europäischen Marktführer für Zahlungsverkehrs- und Transaktionsdienste. Mit innovativen Technologien, umfassender digitaler Kompetenz und tiefgreifendem Branchenwissen begleitet Atos die digitale Transformation von Kunden aus unterschiedlichen Marktsegmenten: Banken, Bildung, Chemie, Energie und Versorgung, Gesundheit, Handel, Medien und Verlage, Öffentlicher Sektor, Produktion, Telekommunikation, Transport und Logistik, Versicherungen und Verteidigung.
Der Konzern ist der weltweite IT-Partner der Olympischen und Paralympischen Spiele. Atos firmiert unter den Marken Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify und Worldline. Atos SE (Societas Europaea) ist an der Pariser Börse als eine der 40 führenden französischen Aktiengesellschaften (CAC40) notiert.

www.atos.net

Anleitung zur Deaktivierung der beA-Software auf Windows-Computern

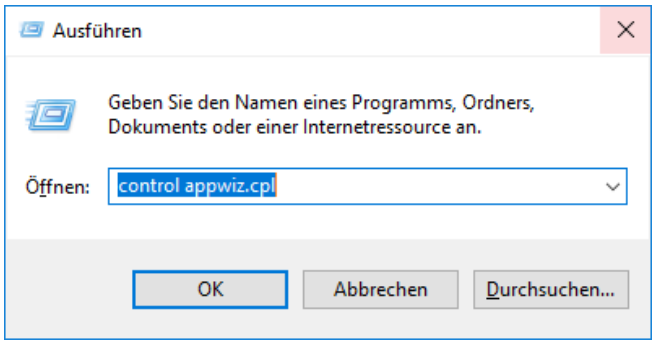
Sie können die beA-Software auf Ihrem Windows-Computer deaktivieren, indem Sie die beA-Client Security deinstallieren (Variante 1) oder indem Sie sie aus dem Autostart entfernen (Variante 2).

Variante 1: Deinstallation beA ClientSecurity unter Windows

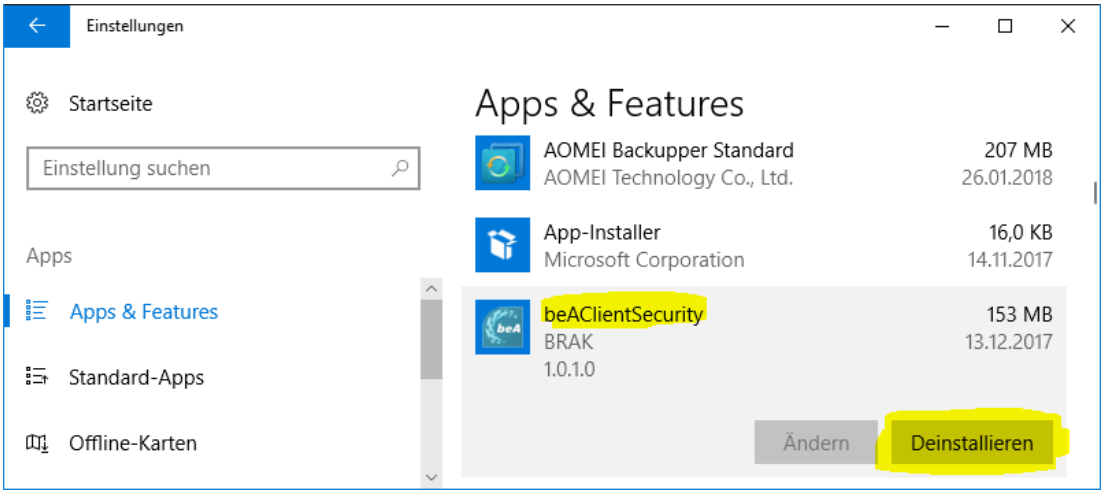
Um die beA ClientSecurity unter Windows zu deinstallieren, starten Sie die Anwendungsverwaltung durch Navigation in der Startleiste:

Start → Einstellungen → Apps & Features

Alternativ können Sie die Anwendungsverwaltung ebenfalls aufrufen, wenn Sie gleichzeitig die **Windowstaste und R** drücken. Anschließend öffnet sich ein Eingabefenster, in das „control appwiz.cpl“ eingegeben wird:



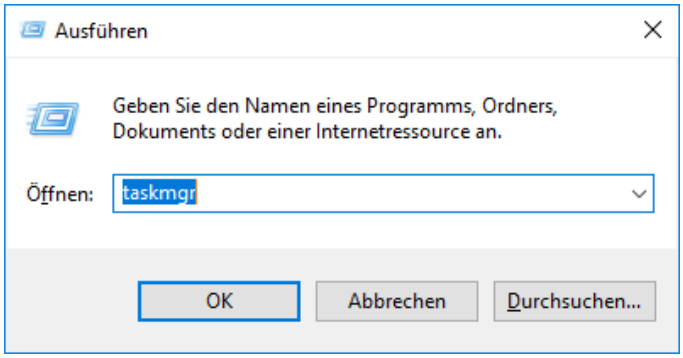
In der Anwendungsverwaltung wählen Sie den Eintrag „beaClientSecurity“ aus und betätigen anschließend die Schaltfläche „Deinstallieren“. Folgen Sie den Anweisungen auf dem Bildschirm.



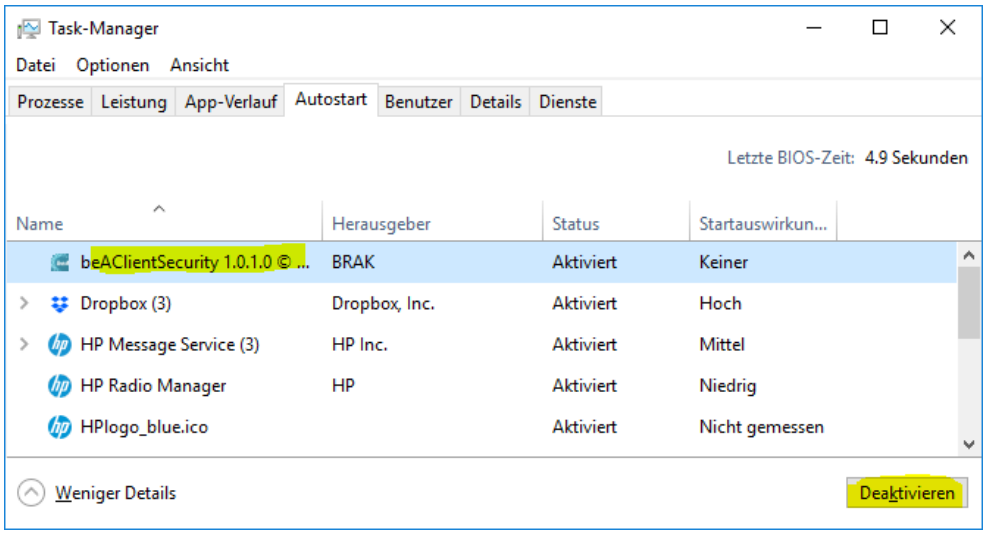
Variante 2: Entfernen der beA ClientSecurity vom Autostart unter Windows

Wollen Sie lediglich den Autostart der beA ClientSecurity verhindern, jedoch die Applikation auf Ihrem Rechner belassen, dann folgen Sie dieser Anleitung.

Starten Sie den Taskmanager, indem Sie gleichzeitig die **Windowstaste und R** drücken. Anschließend öffnet sich ein Eingabefenster, in das „taskmgr“ eingegeben wird:

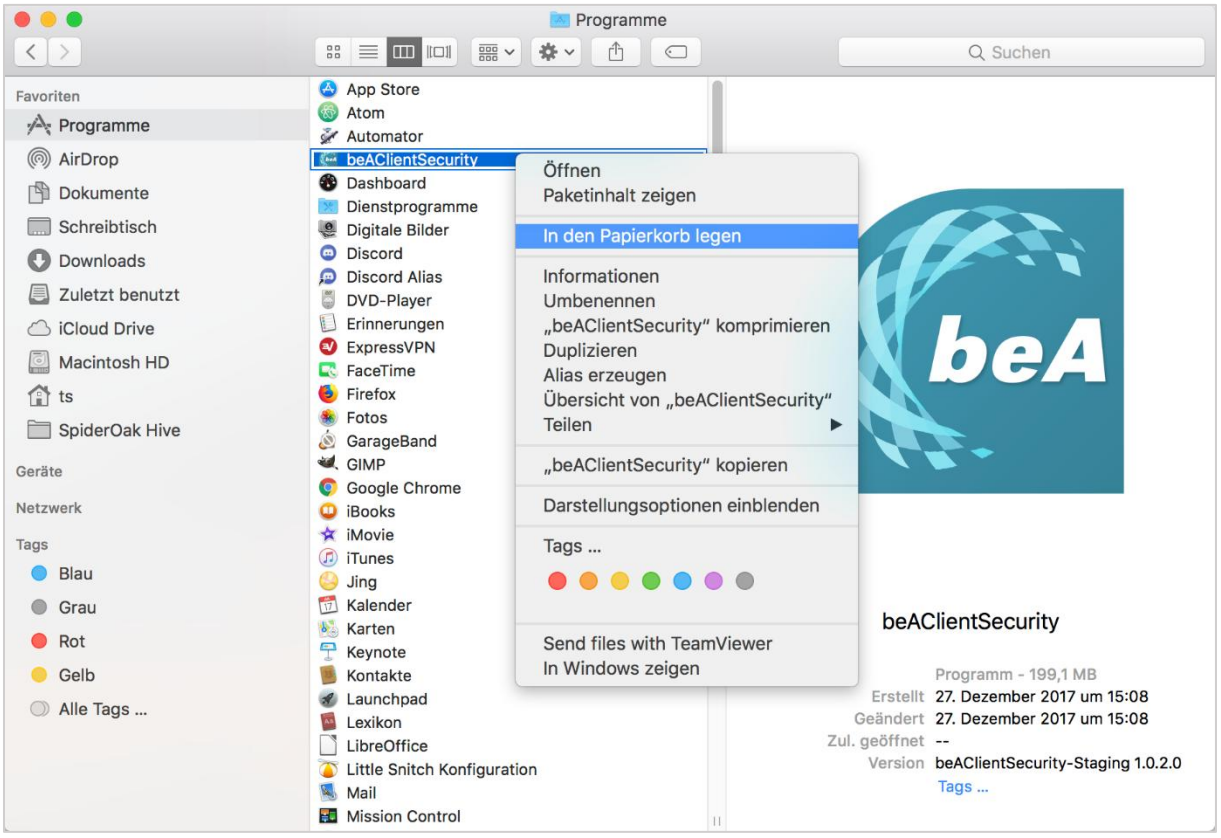


Im nun angezeigten Dialog wählen Sie den Reiter „Autostart“ aus. Suchen Sie den Listeneintrag „beAClientSecurity“ und deaktivieren Sie ihn. Die Software startet nun nicht mehr automatisch.



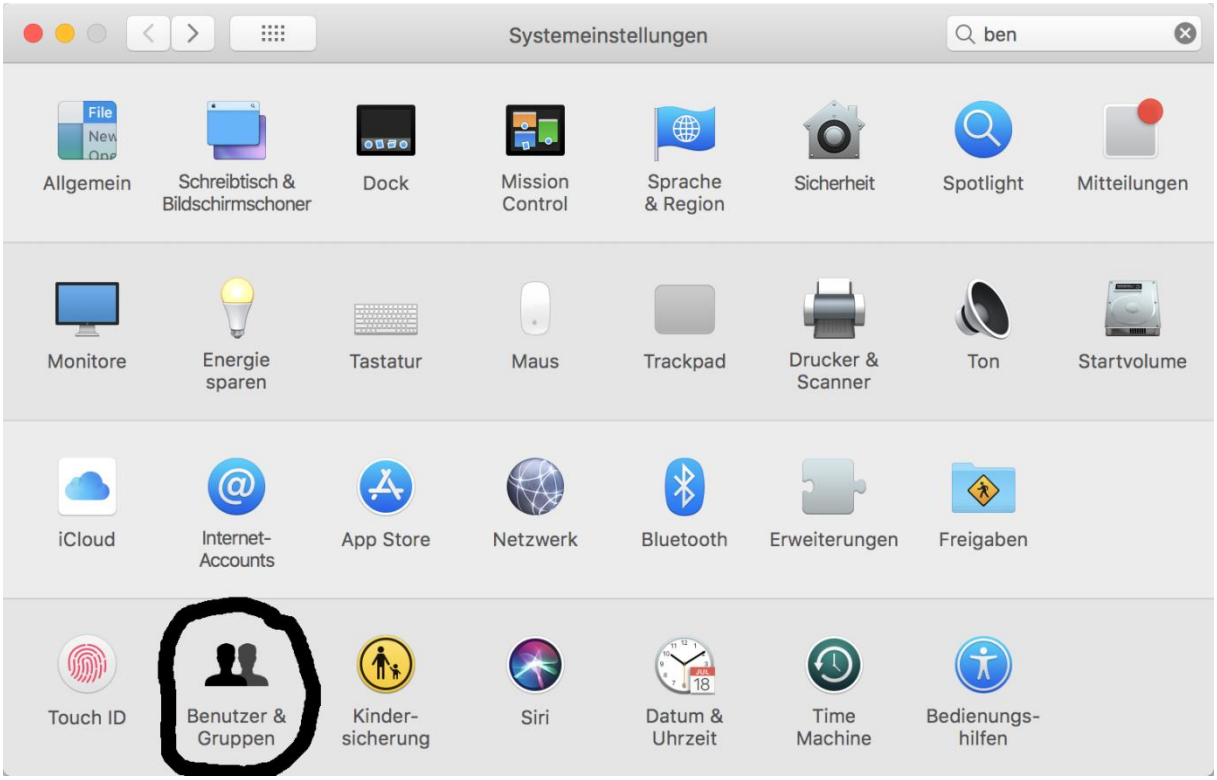
Deinstallation der beA-Software unter MacOS und Entfernen aus dem Autostart

Bei der Standard-Installation der beA-Software wird die ClientSecurity-Programmdatei in den Ordner *Programme* kopiert. Finden Sie die Datei mit dem Namen *beAClientSecurity* im Ordner *Programme* und wählen Sie mittels Kontextmenu (Rechtsklick) die Option *In den Papierkorb legen* aus. Ggf. müssen Sie nun Ihr Administratorkennwort eingegeben.



Die ClientSecurity-Komponente ist damit deinstalliert. Um sicherzugehen, dass das Programm nicht im Autostart vorhanden ist (was nicht standardmäßig aktiviert ist), können Sie in den Systemeinstellungen nachschauen:

Rufen Sie dazu unter Systemeinstellungen *Benutzer & Gruppen* auf.



Dort dann für den entsprechenden Benutzer den Reiter *Anmeldeobjekte* öffnen und sicherstellen, dass die *beAClientSecurity* dort nicht auftaucht. Falls beAClientSecurity doch auftaucht, diese auswählen und durch einen Klick auf das „-„ Zeichen aus der Liste entfernen.