Verschlüsselungsprogramm o.ä. zum Austausch von Notendateien

Beitrag von „Super-Lion“ vom 24. Januar 2021 22:36

Hallo zusammen,

bei uns in Ba-Wü stehen im Februar die Zeugnisse an.
Nun geht die Frage um, wie wir am besten die Notenlisten austauschen.
Habt Ihr entsprechende Verschlüsselungssoftware oder wie macht Ihr das?

Freue mich über Tipps bzw. einen Austausch.
Für Berichte habe ich früher immer TrueCrypt genommen, aber ich meine, das wird nicht mehr unterstützt.
Vielen Dank und viele Grüße
Super-Lion

Beitrag von „CDL“ vom 24. Januar 2021 22:40

Veracrypt-Container anlegen, Notenliste rein, an KuK senden über Kanal 1 (LMS, Schulmailaccount). Passwort mitteilen über Kanal 2 (Telefonanruf, Nachricht über ThreemaWork). Veracrypt gibt es kostenfrei über die Landesseiten. Die Vorgehensweise wird so empfohlen und wurde uns im Ref vorletztes Jahr so beigebracht. Funktioniert zuverlässig.

Beitrag von „Websheriff“ vom 24. Januar 2021 22:40

passwortgeschützte zip-Datei

Beitrag von „kaQn4p“ vom 24. Januar 2021 22:45

PGP verschlüsselte E-Mail. Öffentliche Schlüssel auf zentraler Lernplattform speichern, von dort herunterladen und importieren, (optional Fingerprint abgleichen) und schon steht die sichere Kommunikation. Stichwort dürfte dann Gpg4win sein.

Beitrag von „kaQn4p“ vom 24. Januar 2021 22:47

Nachtrag: ansonsten eine der anderen Methoden verwenden. Bitte das Passwort nie über den gleichen Kommunikationskanal wie die Datei verteilen.

Beitrag von „Super-Lion“ vom 24. Januar 2021 23:11

> Zitat von Websheriff
>
> passwortgeschützte zip-Datei

Reicht das aus? Ich meine, dass man passwortgeschützte Dateien knacken kann. Oder ist das bei zip-Dateien anders?

Beitrag von „Websheriff“ vom 24. Januar 2021 23:20

interessante Aufstellung:

https://datenschutz-schule.info/themen/e-mail-...-sicher-nutzen/

Beitrag von „Super-Lion“ vom 24. Januar 2021 23:30

> Zitat von Websheriff

> interessante Aufstellung:
>
> https://datenschutz-schule.info/themen/e-mail-...-sicher-nutzen/

Dankeschön! Jetzt bin ich verwirrt.
Wir haben in der Schule Schulmail-Adressen über strato. Könnte man dann darüber Notenlisten verschicken?
Oder ist das wieder von Bundesland zu Bundesland verschieden? Die verlinkte Seite ist ja von NRW und ich bin aus Ba-Wü. ☹

Beitrag von „o0Julia0o“ vom 25. Januar 2021 00:47

Bei uns dürfen Notenkonferenzen per Videochat durchgeführt werden. Das ist von Bundeslang zu Bundesland verschieden.

Win-Rar verschlüsselt ab Version 5.0 mit AES-256 - das ist ausreichend.

Beitrag von „CDL“ vom 25. Januar 2021 05:43

> Zitat von Super-Lion
>
> Dankeschön! Jetzt bin ich verwirrt.
> Wir haben in der Schule Schulmail-Adressen über strato. Könnte man dann darüber Notenlisten verschicken?
> Oder ist das wieder von Bundesland zu Bundesland verschieden? Die verlinkte Seite ist ja von NRW und ich bin aus Ba-Wü. ☹

Wenn das eure offiziellen Schulmailadressen sind, solltet ihr die dafür nehmen können, denn darüber dürft ihr euch ja auch sonst über SuS austauschen. Wenn du ganz sicher sein möchtest, dann frag deine SL per Mail (so bekommst du es schriftlich) ob das rechtlich in Ordnung ist.

Beitrag von „kaQn4p“ vom 25. Januar 2021 06:03

Ich würde, bezogen auf den Link oben, Dinge wie Prüfungen usw. auch niemals innerhalb der selben Domäne unverschlüsselt übertragen. Hier wird in der Regel nur beim Verschicken der Mail verschlüsselt! Auf dem Server liegen die Daten dann meist in Klartext. Daher: wurde der Mailaccount kompromittiert, können die Daten gelesen werden. Wurden diese jedoch mittels PGP verschlüsselt oder befinden sich in einem kennwortgeschütztem Archiv sind sie auch auf dem Server nochmal geschützt.

Beitrag von „Kalle29“ vom 25. Januar 2021 10:57

PGP - großer Fan davon, für 98% der Bevölkerung leider nicht nutzbar 

Am ehesten funktioniert da wohl noch die ZIP-Verschlüsselung, die ist relativ idiotensicher. Hab aber gerade keine Ahnung, womit genau die verschlüsselt.

Beitrag von „Philio“ vom 25. Januar 2021 12:43

> Zitat von Super-Lion
>
> Reicht das aus? Ich meine, dass man passwortgeschützte Dateien knacken kann. Oder ist das bei zip-Dateien anders?

7-Zip kann mit AES-256 verschlüsseln, das ist der derzeitige Industriestandard. Aber grundsätzlich kann jede Verschlüsselung geknackt werden, das ist nur eine Frage des Aufwands. Aber ohne deine dienstliche Verordnung zu kennen, vermute ich, dass du nur dafür sorgen musst, dass die Verschlüsselung „hinreichend sicher“ ist. Dass die Verschlüsselung durch Profi-Hacker oder die NSA nicht knackbar ist, erwartet keiner.

Beitrag von „Philio“ vom 25. Januar 2021 13:07

Was noch nicht erwähnt wurde: ProtonMail. ProtonMail hat eine Freemail-Variante, die für den Normaluser völlig ausreichend ist und Ende-zu-Ende-Verschlüsselung der Mails bietet. Ob ihr

das rechtlich nutzen dürft kann ich nicht sagen - die Server von ProtonMail sind ausserhalb der EU.

Beitrag von „kaQn4p“ vom 25. Januar 2021 13:31

> Zitat von Philio
>
> die Server von ProtonMail sind ausserhalb der EU

Protonmail kannte ich noch nicht, danke dafür. Aber der Datenschutzbeauftragte wird es wohl auf Grund des Serverstandorts killen^^

Beitrag von „CDL“ vom 25. Januar 2021 15:04

> Zitat von Kalle29
>
> PGP - großer Fan davon, für 98% der Bevölkerung leider nicht nutzbar ☹
>
> Am ehesten funktioniert da wohl noch die ZIP-Verschlüsselung, die ist relativ idiotensicher. Hab aber gerade keine Ahnung, womit genau die verschlüsselt.

Veracrypt ist super, ehrlich. Nicht komplett idotensicher, aber man kommt, wenn man die Bild-Anleitung des Landes BW befolgt innerhalb weniger Minuten zuverlässig zurecht damit.

Beitrag von „Philio“ vom 25. Januar 2021 15:30

D'accord VeraCrypt ist super, aber für das Versenden einer einzelnen Datei fast schon mit Kanonen auf Spatzen geschossen - zumal die Datenweitergabe nicht der intendierte Use Case für VeraCrypt ist, sondern eigentlich die Verschlüsselung von Daten, die beim Nutzer verbleiben um zum Beispiel zu verhindern, dass beim Verlust eines Datenträgers oder Endgeräts die Daten in falsche Hände fallen.

Beitrag von „CDL“ vom 25. Januar 2021 15:42

> Zitat von Philio
>
> D'accord VeraCrypt ist super, aber für das Versenden einer einzelnen Datei fast schon mit Kanonen auf Spatzen geschossen - zumal die Datenweitergabe nicht der intendierte Use Case für VeraCrypt ist, sondern eigentlich die Verschlüsselung von Daten, die beim Nutzer verbleiben um zum Beispiel zu verhindern, dass beim Verlust eines Datenträgers oder Endgeräts die Daten in falsche Hände fallen.

Stimmt, aber wenn man es dann eh schon auf dem Rechner installiert hat, um seine Notendateien (etc.) zu verschlüsseln, dann kann man es halt auch für die schnelle Datenweitergabe im Kollegium nutzen.

Beitrag von „Kalle29“ vom 25. Januar 2021 16:32

> Zitat von CDL
>
> Veracrypt ist super, ehrlich. Nicht komplett idotensicher, aber man kommt, wenn man die Bild-Anleitung des Landes BW befolgt innerhalb weniger Minuten zuverlässig zurecht damit.

Ich nutze das Ding auch zur Verschlüsselung meiner in der Schule gelagerten Backupfestplatte (ihr wisst ja: ein Backup außer Haus lagern) :-). Allerdings wisst ihr ja, dass ich seit längerem die schulische IT betreue und seid mir versichert: Nicht mal das Schließen eines Programms mit dem "X" ist idiotensicher

---

Beitrag von „Philio“ vom 25. Januar 2021 16:36

> Zitat von Kalle29
>
> Nicht mal das Schließen eines Programms mit dem "X" ist idiotensicher

O-Ton: "Wozu brauche ich OneNote, ich habe doch Teams"... Stimmt, wozu brauche ich einen Schraubenzieher, ich habe doch einen Hammer 😛

Beitrag von „s3g4“ vom 26. Januar 2021 17:00

> Zitat von Philio
>
> 7-Zip kann mit AES-256 verschlüsseln, das ist der derzeitige Industriestandard. Aber grundsätzlich kann jede Verschlüsselung geknackt werden, das ist nur eine Frage des Aufwands. Aber ohne deine dienstliche Verordnung zu kennen, vermute ich, dass du nur dafür sorgen musst, dass die Verschlüsselung „hinreichend sicher“ ist. Dass die Verschlüsselung durch Profi-Hacker oder die NSA nicht knackbar ist, erwartet keiner.

> Zitat von scrambox
>
> On average, to brute-force attack AES-256, one would need to try 2^{255} keys. (This is the total size of the key space divided by 2, because on average, you'll find the answer after searching half the key space.)
>
> So the time taken to perform this attack, measured in years, is simply 2^{255} / 2,117.8 trillion.
>
> Expressed as an exponent of 10, that's $2.73 * 10^{61}$. Written in full format:
>
> 27,337,893,038,406,611,194,430,009,974,922,940,323,611,067,429,756,962,487,493,203 years.

Die Zeit ist niemandem eine Notenliste wert. 😆

Beitrag von „Super-Lion“ vom 1. Februar 2021 18:04

Danke mal für alle Eure Antworten.
Ich harre jetzt 'mal der Dinge, was von "oben" beschlossen wird.
Im Moment sind wir wieder bei der Papierform.

Beitrag von „Seph“ vom 1. Februar 2021 21:39

Ich nutze auch grundsätzlich Veracrypt. Das funktioniert super schnell, ist unkompliziert, belastet die Systemressourcen kaum und ist sicher...jedenfalls dann, wenn man nicht einen auf "DAU" macht und eine AES-256 Verschlüsselung mit einem Passwort wie "123456" absichert.

Beitrag von „CDL“ vom 1. Februar 2021 22:26

Hey Wer hat dir mein Passwort verraten?!?  Du Hacker du.  (Bestimmt heimlich mitgefilmt beim Eintippen. *Aluhut grade rück und Julia channel* )

Beitrag von „Seph“ vom 1. Februar 2021 23:19

Das belegt seit Jahren in schöner Regelmäßigkeit einen der vordersten Plätze in der Liste der meistgenutzten Passwörter (in verschiedenen Variationen sogar mehrere der vordersten Plätze). Dicht gefolgt von Klassikern wie "password", "picture1", "qwerty" und natürlich "admin". 

Die Abarbeitung dieser Liste kommt noch vor der Anwendung eines Wörterbuchangriffs, der ebenfalls schnell gemacht und relativ erfolgversprechend ist oder Social Engineering....habe ich mal gehört 

Beitrag von „Kiggie“ vom 2. Februar 2021 07:44

Unsere Schüler regen sich immer auf 'Bäh, ich muss ja Sonderzeichen und eine Zahl beim Passwort nutzen' 

Beitrag von „Kalle29“ vom 2. Februar 2021 08:50

> Zitat von Seph
>
> Ich nutze auch grundsätzlich Veracrypt. Das funktioniert super schnell, ist unkompliziert, belastet die Systemressourcen kaum und ist sicher...jedenfalls dann, wenn man nicht einen auf "DAU" macht und eine AES-256 Verschlüsselung mit einem Passwort wie "123456" absichert.

Gelegentlich löse ich private PC-Probleme an Laptops von KuK (ja, Schande über mich). Du glaubst gar nicht, was die alles für Passwörter haben - im Regelfall ist es ein Wort und maximal noch 12 hinten dran gehängt.

Beitrag von „Seph“ vom 2. Februar 2021 09:17

Doch, das glaube ich aufs Wort und das deckt sich leider auch mit meinen Erfahrungen. Gerade deshalb hatte ich das oben halb im Scherz angesprochen.

Beitrag von „Kalle29“ vom 2. Februar 2021 09:32

Ich weiß 

Beitrag von „helmut64“ vom 2. Februar 2021 09:55

> Zitat von Philio
>
> grundsätzlich kann jede Verschlüsselung geknackt werden

> Stimmt nicht. Google mal nach "one time pad".
>
> Auch eine astronomische Anzahl möglicher Schlüssel ist keine Sicherheitsgarantie. Bestes Beispiel dafür ist die ENIGMA.

Beitrag von „Seph“ vom 2. Februar 2021 10:14

> Zitat von helmut64
>
> Stimmt nicht. Google mal nach "one time pad".
>
> Auch eine astronomische Anzahl möglicher Schlüssel ist keine Sicherheitsgarantie. Bestes Beispiel dafür ist die ENIGMA.

Das OTP ist leider auch nur dann sicher, wenn alle Nebenbedingungen peinlich genau eingehalten werden, was in der Praxis ziemlich unhandlich ist, insbesondere zur Verschlüsselung größerer Datenmengen. Aber stimmt schon, damit hat man theoretisch ein unbrechbares Verfahren an der Hand.

Die Enigma hatte so deutliche kryptografische Schwächen, dass mir noch immer unklar ist, wie das bei der Konstruktion nicht auffallen konnte. Alleine die Umkehrwalzen führen zu einer Schwächung um etwa 13 Größenordnungen. Blöd war auch, dem Konzept "Security through obscurity" zu folgen. Den Fehler macht Deutschland teils immer noch. Ich selbst bin Fan des Kerkhoff´schen Prinzips, Standards wie AES sind diesbezüglich gut implementiert und vor allem durch aufwendige Audit-Verfahren auf Sicherheitslücken geprüft.

Übrigens hat man auch bei einfacher monoalphabetischer Substitution eine extreme Anzahl möglicher Schlüssel, gleichzeitig ist das Verfahren sehr leicht angreifbar.