Umsetzung Dienstanweisung personenbezogene Daten NRW (und andere Bundesländer?)

Beitrag von „TwoEdgedWord“ vom 25. März 2018 08:19

Da anscheinend die IT-Apokalypse in der Schule dämmert rege ich eine Diskussion an, wie mit der Dienstanweisung

https://www.schulministerium.nrw.de/docs/Recht/Dat...eisungRdErl.pdf

an den einzelnen Schulen umgegangen wird.

Erfahrungsberichte, Best-Practices, fundierte rechtliche Einschätzungen sind gerne gesehen, Rants, Grundsatzdiskussionen und Ausgüsse über die Rückständigkeit des Schuluniversums bitte nur in homöopatischen Dosen zur Auflockerung und allgemeinen Erheiterung.

Insbesondere wäre interessant, inwieweit der bisherige Ansatz (= Ignorieren) weiterhin trägt.

Beitrag von „TwoEdgedWord“ vom 25. März 2018 08:30

Nachtrag:

Eine Synopse zwischen aktueller und ersetzter Version wäre sehr schön. Falls jemand dazu was beitragen kann....

Beitrag von „plattyplus“ vom 25. März 2018 08:58

Warum soll das eine Apokalypse werden? DIe Daten werden doch schon seit mindestens 10 Jahren elektronisch verarbeitet. Oder habt ihr nicht die SchiLD-Software im Einsatz?

--> https://www.svws.nrw.de/index.php?id=schildnrw

Was mir derweil etwas Bauchschmerzen bereitet ist die fehlende Hardware-Trennung zwischen Verwaltungs- und Schulnetz. Früher waren das wirklich zwei getrennte Netze. Heute hängt das alles über einen Router mit Firewall zusammen. Hoffentlich sind dessen Programmierung

ausreichend fehlerfrei und die Paßwörter gut genug.

Beitrag von „Kalle29“ vom 25. März 2018 11:38

Ich sehe das auch alles kritisch. Das neue Datenschutzrecht ist sehr streng und mir persönlich ist völlig unklar, wie das an Schulen umgesetzt wird. Zum Glück bin ich kein Schulleiter. Aber an jeder Schule werden personenbezogene Daten in irgendeiner Art und Weise verarbeitet. Dafür muss (meiner Meinung nach) eine hieb-und stichfeste Datenschutzerklärung vorhanden sein. Ich bezweifel, dass dies an den meisten Schulen vorhanden ist. Viele Schulen bieten irgendwelche Dienste, beispielsweise Krankmeldungen oder Newsletter, auf ihren Homepages an. Da werden personenbezogene Daten erhoben. Unsere Windows-Server speichert beispielsweise Login-Zeiten von Schülern an den Rechnern sowie deren Nutzung. Ziemlich sicher sind das personenbezogene Daten.

Die Verarbeitung von Daten in Schild halte ich dagegen fast für unkritisch.

Beitrag von „plattyplus“ vom 25. März 2018 11:55

> Zitat von Kalle29
>
> Unsere Windows-Server speichert beispielsweise Login-Zeiten von Schülern an den Rechnern sowie deren Nutzung. Ziemlich sicher sind das personenbezogene Daten.

Moin,

die Logins halte ich für unkritisch so lange aus dem Login ohne zusätzliche Listen nicht auf die Person dahinter geschlossen werden kann. An der Schule, an die ich abgeordnet bin, haben alle (auch die Schüler) Logins in der Form Nachname.Vorname. Da sehe ich Dein Problem in ganzer Schärfe.

Was SchiLD und die Datenerfassung angeht, sehe ich das weitaus kritischer, weil dort mitunter wirklich heiße Daten hinterlegt sind, z.B. die Krankenakte der Schüler (Atteste werden eingetragen). Meiner Meinung ist es da mit einer Datenschutzerklärung nicht getan. Sehr viele Kollegen werden die unterschreiben und dann trotzdem weitermachen, weil sie potentielle Gefahren gar nicht erkennen, insb. was den Umgang mit ihren privaten Geräten angeht.

Und nein, wenn ich die Schülernoten bei mir auf dem Notebook oder Tablet habe, darf ich dieses Tablet eben nicht mehr im Klassenraum an den Beamer hängen. Aber erklär das mal den fachfremden Kollegen.

Also wenn Du es nagelfest machen willst, reicht so eine Dienstanweisung meiner Meinung nach nicht aus. Dann muß ganz klar das System zur Datenverarbeitung aus einer Hand vom Schulministerium gestellt und administriert werden, so daß alle Nutzer (und die Schulleitung ist dann auch Nutzer) sich um den Datenschutz keine Gedanken mehr machen müssen. Ich traue jedenfalls den "normalen" Schulleitern im Üblichen nicht zu, daß sie das alles überblicken, wenn sie nicht gerade vorher selber Informatik unterrichtet haben.

Beitrag von „Kalle29“ vom 25. März 2018 12:46

Bei uns sind die Logins (historisch) auch Vorname.Nachname. Der Zugang zum Server an sich ist natürlich beschränkt (ausschließlich ich). Das hilft aber natürlich nix, weil ich die Daten auch einsehen kann, wenn kein akuter Vorfall vorhanden ist, der Recherche benötigt. Die Idee, eine Liste zu führen, auf der anonymisierte Logins gespeichert sind und diese dann beispielsweise bei der Schulleitung zu hinterlegen, könnte das Problem entschärfen. Spannenderweise gab es an unserer Schule noch überhaupt keine Infos zur neuen Datenschutzverordnung. Ich habe da nach dem Konsum einer aktuellen ct mal einige Leute drauf aufmerksam gemacht, aber offenbar wird das Problem nicht als ernst gesehen.

Die Datenverarbeiten auf privaten Geräten wird natürlich genauso weiter gehen wie sie es bisher gegangen ist. Da interessiert sich keiner für - so hart es ist. Wenn ich mich recht entsinne, waren die Anforderungen an korrektes Verarbeiten in NRW auch so unpraktisch, dass sie nicht umsetzbar sind. Nicht mein Problem, ich bin immer noch in der guten alten Papierwelt unterwegs.

Bei Schild nehme ich naiverweise an, dass dort hoffentlich ein Datenschutzbeauftragter mal drüber geschaut hat. Bei unserer Datenschutzbestimmung auf unserer Homepage hat das sicherlich keiner gemacht. Auch unsere Datenschutzvereinbarung für die Nutzung der schulischen IT durch die Schüler erscheint mir eher mit der heißen Nadel gestrickt. Eine Kollegin hat bei der Einführung von Moodle mal versucht, den Datenschutzbeauftragen des Schulträgers dazu zu bekommen, eine saubere Vereinbarung zur Verfügung zu stellen. Ist natürlich nicht geschehen. (Moodle - halte ich fast noch für kritischer als unseren Server, denn dort sind auch sämtliche Login-Daten für die Moodle-Admins einsehbar).

Beitrag von „kleiner gruener frosch“ vom 25. März 2018 13:01

Schild - da es eine Anwendung ist, die vom Ministerium zur Verfügung gestellt wurde, gehe ich mal davon aus, dass es datenschutzrechtlich abgesegnet ist. Wäre komisch, wenn nicht. (Ich muss aber zu meiner Schande gestehen, dass ich das bisher immer automatisch vorausgesetzt habe. Ich werde es mal hinterfragen.)

Private Daten: die neue Erklärung für die Kolleginnen macht ziemlich viel Wirbel. Verständlicherweise. Ich muss mal in Ruhe schauen, was es da genau neues gibt . Denn eine entsprechende Datenschutzerklärung gibt es ja schon seit Jahren. Die haben auch alle Kolleginnen ohne Widerstand unterschrieben. Ich kann den Widerstand der Kolleginnen und der Gewerkschaften im aktuellen Fall aber schon verstehen. Stimme da Kalle29 zu. Die Anforderungen sind für die Arbeit zuhause nur schwer 100%-ig umzusetzen.

Pädagogisches / Verwaltungsnetz: mich wundert ehrlich gesagt, dass sich das noch nicht durchgesetzt hat, dass es in der Schule 2 verschiedene, voneinander strikt getrennte Netzwerke gibt.

Ich halte den Datenschutz aber schon für wichtig. Auch wenn er schwierig umzusetzen ist.

kl. gr. frosch

Beitrag von „plattyplus“ vom 25. März 2018 13:06

> Zitat von kleiner gruener frosch
>
> Pädagogisches / Verwaltungsnetz: mich wundert ehrlich gesagt, dass sich das **noch nicht** durchgesetzt hat, dass es in der Schule 2 verschiedene, voneinander strikt getrennte Netzwerke gibt.

Er setze "noch nicht" durch "nicht mehr" und Du weißt, wie es läuft. Früher hatten wir das alles schön getrennt, heute geht das aus irgendwelchen Gründen nicht mehr und alle Kollegen wundern sich, warum sie auf dem SchiLD-Rechner auf einmal google.de öffnen können.

Beitrag von „kodi“ vom 25. März 2018 16:29

Naja, was hat sich geändert:

- Der Schulleiter muss nun stichprobenhaft kontrollieren.
- Das Auskunftsrecht wurde in den Erlaß übernommen.

Alles andere galt vorher doch auch schon, wenn nicht über den alten Erlaß, dann über die entsprechenden Gesetze.

Beitrag von „kleiner gruener frosch“ vom 25. März 2018 16:37

Danke, kodi. Ich nutze die Ferien dennoch mal, um mich da nochmal genauer einzulesen. Sitze morgen eh nutzlos in der Schule herum, während ich auf die Fensterputzer warte. Da habe ich genug Zeit und Langeweile.

kl. gr. frosch

Beitrag von „Kalle29“ vom 25. März 2018 17:24

Kannst du uns deine Erkenntnisse mitteilen? Ich bin auch interessiert. Zum Glück scheint die gesamte Verantwortung nicht delegierbar bei der Schulleitung zu liegen.

Edit: Ich hab das Gefühl, dass in NRW da nicht mal das Ministerium richtig drüber nachdenkt oder das die ct (Ausgabe 5/18) Quatsch erzählt.

Minsteriumswebseite, darunter dann ct 5/18 (bin zu blöde, das richtig zu formatieren)

> Zitat
>
> Beim Einsatz elektronischer Verarbeitungsprozesse werden Daten wie z. B. Protokolldaten über Loginzeiten an Lernplattformen oder die IP-Adressen angemeldeter Endgeräte erhoben bzw. generiert. Diese Daten dienen der Gewährleistung von Systemintegrität und Revisionsfähigkeit der infomationstechnischen Systeme gemäß DSG NRW3. Grundlage zur Erhebung dieser Daten ist also nicht das Schulgesetz. Die pädagogische Nutzung von Protokolldaten ist somit für die Schule unzulässig.

> Zitat

> Beim Website-Betreiber kann das beispielsweise das Interesse an der Betriebssicherheit seiner Homepage sein. Um Angriffe erkennen und abwehren zu können, dürfen sie dafür die IP-Adressen der Besucher für kurze Zeit speichern. Auf die Dauer der Speicherung, die im Falle von IP-Adressen nicht länger als 14 Tage betragen sollte, muss er seine Besucher wiederum in der Datenschutzerklärung hinweisen

Mag sein, dass die Speicherung zulässig ist. Aber ich vermisse einen Hinweis, dass dies in der Datenschutzverordnung der Webseite hinterlegt werden muss. Außerdem fallen diese Daten ja auch an unseren pädagogischen Schulsystem an.

Beitrag von „kodi“ vom 25. März 2018 18:06

Ich bezieh mich im folgenden nur auf den für normale Lehrer relevanten Teil (DV auf privaten Endgeräten):

Dazu gibt es von der GEW hier findet sich eine kurze Info der GEW zum Thema.

Wir haben den DV-Antrag wie in einer GEW-Rundmail empfohlen um diesen Passus ergänzt:

> Zitat
>
> **Ich weise darauf hin, dass ich kein ausgebildeter IT-Spezialist bin und deshalb nicht alle geforderten Maßnahmen für mein privates Gerät bis ins Detail überblicken kann und somit jegliche persönliche Haftung ausschließe.**

Ob das im Zweifelsfall eine rechtliche Wirkung hat, ist bisher unklar.

Was heißt der Antrag für den normalen Lehrer?

- Keine Datenverarbeitung auf privaten Geräten ohne Genehmigung.
- Nur die Daten verarbeiten, die explizit im Antrag stehen.
- Eigenes Benutzerkonto für Schuldaten
- Aktuelles Betriebssystem auf aktuellem Sicherheitsstand.
- Firewall und Virsenscanner, sofern nicht im Betriebssystem intesgriert, wie z.B. bei Win10.
- Bildschirmsperre einrichten
- USB-Datenträger verschlüsseln <-- *Hauptproblem in meinem Kollegium*

- Backups machen
- Löschfristen einhalten. Am besten durch entsprechende Datenorganisation: Ordner mit Schuljahr, den man dann löschen kann (auch aus Backups).
- Cloudbackup für Schulbenutzerkonto abstellen
- Bei Handy/Tableteinsatz: Keine Schulkommunikation per WhatsApp und Co. Keine Schultelefonnummern (Eltern/Schüler) ins Adressbuch übernehmen, solange WhatsApp und Co darauf Zugriff haben. Cloudbackup ausstellen.

Den DV-Antrag als Word-Datei hat dankenswerterweise ein Kollege hier im Schild-Forum bereit gestellt. Das Ministerium stellt natürlich mal wieder nur ein PDF bereit.... O_o

---

Beitrag von „Bolzbold“ vom 25. März 2018 19:40

Der PhV beschwert sich auch über die neuen Vorgaben.
Ich finde die Vorgaben einerseits in Teilen sinnvoll, andererseits aber praxisfern, weil es zu viele digital Dummies unter den Kollegen gibt.
Mein Gerät würde - mit Ausnahme des USB-Sticks, den ich aber für die Datenübermittlung in der Regel nicht verwende - alle Vorgaben erfüllen. Mal sehen, ob unsere SL demnächst alle Kollegen zur Beantragung der DV-Erlaubnis auf privaten Geräten anweist oder ob doch die rheinische Lösung bevorzugt wird.

Beitrag von „Landlehrer“ vom 25. März 2018 19:50

> Zitat von TwoEdgedWord
>
> Insbesondere wäre interessant, inwieweit der bisherige Ansatz (= Ignorieren) weiterhin trägt.

Wo kein Kläger, da kein Richter. Die Dienstanweisung ist in der Praxis nicht umsetzbar, wenn der Dienstherr keine Vollzeitstelle für die Administration schafft und nicht ausreichend Rechnerarbeitsplätze zur Verfügung stellt.

Beitrag von „Flipper79“ vom 25. März 2018 20:08

V.a. frage ich mich ob der SL ohne rechtliche Grundlage einfach und gegen meinen Willen Einsicht in meine privaten Rechner / digitalen Endgeräte (Laptop, PC, Smartphone, Tablet) nehmen darf (stichpunkthaft kontrollieren). Solange ich ihm freiwillig Einblick gewähre, wäre es rechtlich kein großer Akt. Wenn ich aber sage: "Ich möchte nicht, dass sie in meine Daten (sei es privat, sei es schulisch) Einblick nehmen.": Was dann?
Schließlich darf selbst die Polizei in diese nur dann Einsicht nehmen, wenn zumindest der Verdacht einer Straftat im Raume steht und eine richterliche Genehmigung eingeholt wurde.
Kennt sich mein SL so gut aus, dass er überprüfen kann, ob alle genannten Maßnahmen eingehalten wurden meinerseits? Darf er es - wenn er sich damit nicht auskennt - einfach unseren IT-Admin beauftragen? Der wird sich bedanken.
Was, wenn ich mich weigere irgendeinen PC / Laptop etc. bei ihm anzugeben? (So weit sind wir zum Glück noch nicht!).
Was, wenn ich diese Dienstanweisung unterschreibe (da ich echt davon ausgehe, dass ich die Anforderungen erfülle) und diese Anforderungen dann doch nicht erfüllt sind?
Steht in all diesen Fällen dann eines Tages die Polizei vor meiner Türe oder muss ich dann mit dienstrechtlichen Konsequenzen rechnen? Die Polizei wird sich bedanken! Hat ja auch sonst nix zu tun! Die Bezirksregierung oder irgendwelche Gerichte, die sich möglicherweise mit solchen dienstrechtlichen Konsequenzen beschäftigen müssen, werden sich auch freuen (braucht es doch dann bei der BezReg auch IT-Spezialisten).

Streng genommen müsste man doch dann auch sein Notenbuch in Papierform so sichern, dass dort kein unbefugter hereinschauen kann. Wie sieht das Ganze aus, wenn in der Schule zu bestimmten Terminen offen die Notenlisten im LZ herumfliegen, damit jeder Kollege die Gelegenheit hat die eingetragenen Noten zu kontrollieren und ggf. abzuändern?

Beitrag von „Mikael“ vom 25. März 2018 20:23

Und wie wird so etwas in der "freien" Wirtschaft gehandhabt?

Die Mitarbeiter bekommen von ihrer Firma dienstliche Geräte gestellt (Notebooks, Tablets, Smartphones) die von der Firma zentral datenschutzkonform administriert werden. Da braucht sich keiner Gedanken darüber machen, ob das System dem aktuellen Stand der Technik enspricht.

Nur wir Lehrer lassen uns wieder verar...

Noch ein Grund mehr, die alten bewährten Papierlisten zu führen und personenbezogene Schülerdaten nur an den schulischen Geräten zu verarbeiten. Wenn dann etwas schiefgeht, ist die Schule schuld und nicht der einzelne Kollege.

Gruß !

Beitrag von „Bolzbold“ vom 25. März 2018 23:54

@Mikael

Das wäre bei uns in der Schule mit sage und schreibe drei für alle Kollegen zugänglichen Verwaltungsrechnern logistisch nicht mehr machbar.

Für mich stellt nebenbei die Abkehr vom Papier eine ungeheure Arbeitserleichterung dar - vor allem dann, wenn man mit Software arbeitet, die Notenverwaltung, Kalender und Unterrichtsvorbereitung mit Office-Anbindung kann.
Letztlich wird es sowieso nur so weiterlaufen wie bisher - wo kein Kläger, da kein Richter.

Beitrag von „Mikael“ vom 26. März 2018 01:57

Ich führe meine Notenlisten und schülerbezogenen Notizen nur in Papierform, also ganz datenschutzkonform. Alle halbe Jahr gebe ich dann die Zeugnisnoten in die schulischen PCs ein.

Deshalb brauche ich auch keinen Wisch zu unterschreiben, der dem Dienstherrn Zugriff auf meine privaten PCs erlauben würde.

Gruß !

Beitrag von „TwoEdgedWord“ vom 9. Juni 2018 20:06

Ich bringe das ganze noch mal nach oben. Viel Presse, einige Blogs und Websites haben (temporär) zugemacht, über persönliche Umstellungen von Lehrern habe ich wenig gelesen (und wenn, dann idR Rants über die Rückständigkeit von Datenschutz)

Wie sieht's an eurer Schule inzwischen aus?

- Habt ihr offiziell (Konferenz o.Ä.) drüber gesprochen? Mehr als 3min?
- Wurdet ihr "gezwungen", euch nahegelegt, euch angeboten eine Erklärung zum

datenschutzkonformen Gebrauch privater IT zu unterschreiben? Habt ihr's getan?
- Habt ihr persönlich im schulischen Umgang mit Daten etwas geändert?
- Sitzt ihr/ eure Schulleitung das einfach aus? (So wie einige hier in der Umgebung ....)

Beitrag von „Mikael“ vom 9. Juni 2018 20:59

Bei uns (Nds) gab es Informationen zur neuen DSGVO im Rahmen einer Dienstbesprechung.

Einen Wisch, dass ich schulische, personenbezogene Daten auf meinen privaten PCs verarbeiten darf, habe ich noch nie unterschrieben, da ich keine schulischen, personenbezogenen Daten auf meinen privaten PCs verarbeite.

Wenn der Dienstherr will, dass ich schulische, personenbezogene Daten verarbeite, soll er mir erst einmal einen Dienst-PC stellen und diesen auch datenschutzkonform administrieren, so wie in der "freien" Wirtschaft, dem großen Vorbild für uns "faule Säcke", üblich.

Gruß !

Beitrag von „Zirkuskind“ vom 10. Juni 2018 21:33

Hier (NDS) gab es noch keine Infos. Ich werde Anfang des nächsten Schuljahres unseren neuen Datenschutzbeauftragten befragen.
Persönlich werde ich nächstes Jahr mal wieder analog btw. deutlich weniger digital mit Schülerdaten/Noten arbeiten. Hat aber nichts mit der DSGVO zu tun sondern mit einem neuen System zu tun, das ich ausprobiere.

Beitrag von „Elmorya“ vom 18. Juni 2018 18:45

Hallo,

an unserer Schule sind viele sehr skeptisch gegenüber der Dienstanweisung. Unter anderem wird auch über Notenapps diskutiert. Ich nutze z.B. eine Notenapp, die ich per Bluetooth

synchronisiere und die mit einem Passwort gesichert ist. Folglich habe ich ein Passwort auf dem Handy, dem PC und jeweils für die App. Inwiefern ist so etwas sicher? Kann ich überhaupt garantieren, dass ich bei einer solchen Notenapp die Daten in Sicherheit sind?

Über eine Einschätzung würde ich mich sehr freuen.

Liebe Grüße,

Elmo

Beitrag von „undichbinweg“ vom 18. Juni 2018 18:57

Nein.

Android ist was die Sicherheit angeht ein Desaster. Erfuellt das Passwort die Kriterien eines sicheren Passwortes? Schaetze ich nicht...

Beitrag von „Elmorya“ vom 18. Juni 2018 19:10

Ich würde schon sagen, dass es der Definition eines sicheren Passworts entspricht. Gibt es zu dieser Thematik eine offizielle Aussage o.ä.?

Ich bin diesbezüglich etwas perplex, da es m.E. einfacher ist einen Notenkalender zu klauen, als ein Handy zu hacken. Oder irre ich da so sehr?

Beitrag von „kleiner gruener frosch“ vom 18. Juni 2018 19:23

Nach der alten Erklärung war es eine Grauzone, in der neuen Erklärung sind mobile Geräte explizit erwähnt.
Man kann sie (unter Wahrung der in der Erklärung angegebenen Maßnahmen und Vorgaben (zum Löschen)) nutzen.

Bzgl. Passwort: In der Erklärung wird ein "ausreichend sicheres Passwort" gefordert. Auch in der Handreichung dazu steht nicht mehr. Also: Zahlen, Groß/Kleinbuchstaben, Sonderzeichen, alles schön durchgemischt

kl. gr. frosch

P.S.: speziell bei mobilen Geräten (die machen das halt gerne) solltest du darauf achten, dass die Daten der Notenapp nicht voreingestellt in eine Cloud hochgeladen werden.

Beitrag von „Elmorya“ vom 18. Juni 2018 19:36

Bei meinem Android gehört die besagte App zu den gesperrten Apps (durch ein Antivirenprogramm) und kann nur durch meinen Fingerabdruck oder ein Muster geöffnet werden. Zusätzlich ist ein Passwort in der Notenapp selbst vorhanden. Eine Synchronisation erfolgt bei mir nur per Bluetooth.

Beitrag von „undichbinweg“ vom 18. Juni 2018 20:19

Ich rede nur JETZT nur von der Theorie und gebe nicht meine persönliche Meinung hier wieder:

Android ist ein offenes System, sprich man kann über ans Dateisystem kommen. Wenn man die App mit Fingerabdruck aufmacht, ist die Datenbank verschlüsselt oder nur die App?
Welche andere Apps haben Zugriff aufs Dateisystem? Können diese ggfs. auf die ggfs. nicht verschlüsselte Datenbank kommen?
Cloud? Sync?

Als Informatiker könnte ich Unmengen an Möglichkeiten auflisten...

Beitrag von „plattyplus“ vom 18. Juni 2018 20:21

Du brauchst gar nicht ans Programm selber kommen. Es reicht ein anderes Programm, das regelmäßig Screenshots per Internet an einen Server schickt, um alle anderen Programme auszuspionieren.

Beitrag von „kleiner gruener frosch“ vom 18. Juni 2018 20:23

Sagst du einmal, welche Apps du benutzt?

undichbinweg: den Cloud-Sync muss er abstellen.

kl. gr. frosch

Beitrag von „Elmorya“ vom 18. Juni 2018 20:27

> Zitat von calmac
>
> Ich rede nur JETZT nur von der Theorie und gebe nicht meine persönliche Meinung hier wieder:
>
> Android ist ein offenes System, sprich man kann über ans Dateisystem kommen. Wenn man die App mit Fingerabdruck aufmacht, ist die Datenbank verschlüsselt oder nur die App?
> Welche andere Apps haben Zugriff aufs Dateisystem? Können diese ggfs. auf die ggfs. nicht verschlüsselte Datenbank kommen?
> Cloud? Sync?
>
> Als Informatiker könnte ich Unmengen an Möglichkeiten auflisten...
>
> Die Datenbank der App ist verschlüsselt und erlaubt keinen Zugriff durch fremde Apps. Der Fall eines Virus, der Screenshots erstellt, kann natürlich eintreten. Allerdings habe ich zumindest einen Antivirenschutz.
>
> Meine persönliche Meinung:
>
> Ich denke, dass ich alles tue, um die Daten zu schützen. Wenn jemand mich wirklich hacken will und dazu in der Lage ist, wird er das auch tun. Allerdings empfinde ich es als noch einfacher einen Lehrerkalender zu klauen. Ob man da bald einen Tresor zu

> Hause braucht? 
>
> Letztlich geht es ja auch darum, ab wann man der Dienstanweisung entsprechend handelt. Mehr fällt mir tatsächlich nicht ein, um die Daten zu schützen.
>
> PS: Die Cloud-Synch ist aus. Der Datenaustausch zwischen Laptop und Handy erfolgt per Bluetooth.
>
> PPS: Teacherstudio soll bald genutzt werden. Noch nutze ich Notenbox.
>
> Alles anzeigen

Beitrag von „kleiner gruener frosch“ vom 18. Juni 2018 20:40

Notenbox:

> Zitat
>
> Auf dem mobilen Gerät, also in der NotenBox-App für Android, der NotenBox-App für iPad/iPhone und der NotenBox Windows Store App, sind die Daten AES256 verschlüsselt. Sie werden in der NotenBox für iPad/iPhone so gekennzeichnet, dass sie nicht in der iCloud gesichert werden. Auch die Klassen der NotenBox für Android und der NotenBox Windows Store App sind in einem eigenen Ordner von uns gespeichert, der nicht für eine Sicherung bei Google oder Microsoft vorgesehen ist.

Okay.

Teachertool:

> Zitat
>
> Sämtliche von TeacherTool auf dem Festspeicher dauerhaft abgelegten personenbezogenenDaten von Schülern werden grundsätzlich und ausnahmslos mit dem Algorithmus AES-256symmetrisch verschlüsselt (symmetrisch bedeutet, dass zum Ver- und Entschlüsseln dergleiche Schlüssel benutzt wird). Die Daten werden

> ausschließlich beim Laden durch dieSoftware entschlüsselt (diese benutzt dazu Betriebssystemfunktionen).

Passt.

<off-topic>
Soll es teachertool demnächst auch für Android geben? Oder wechselst du auch das mobile Gerät?

kl. gr. frosch

Beitrag von „Elmorya“ vom 18. Juni 2018 20:59

Ich meinte Teacherstudio und nicht TeaherTool. Bin seit jeher Androide

---

Beitrag von „Valerianus“ vom 19. Juni 2018 06:36

Tapucate verschlüsselt auch und arbeitet komplett offline, das größte Problem bei Android dürften die mangelhaften OS-Updates seitens der Gerätehersteller darstellen. Ich bin froh, dass ich seit neuestem 8.0 mit Patchlevel Juni 2018 habe, aber der Großteil der Geräte dürfte ohne Sicherheitsupdates bei Android 5 oder 6 rumkrabbeln...

Beitrag von „plattyplus“ vom 19. Juni 2018 14:59

> Zitat von Valerianus
>
> das größte Problem bei Android dürften die mangelhaften OS-Updates seitens der Gerätehersteller darstellen

Und genau das war auch für mich das KO-Kriterium gegen Android und fürs iPhone.

Beitrag von „Morse“ vom 19. Juni 2018 18:09

Über Noten-Apps:

Ich habe vollstes Verständnis dafür, dass man als Lehrer besseres zu tun hat, als sich über dubiose Dienstanweisungen den Kopf zu zerbrechen.
RPs, die zentrale Datenschutz-Beauftragte einzelnen Schulen zuordnen, weil sich dort niemand mehr findet, der diesen Job machen will, zeigen, dass hier etwas schief läuft.

Aber: Noten-Apps von kommerziellen Anbietern, bei denen niemand weiß was drin steckt - das ist für mich datenschutzmäßig der Super-GAU!
Dass ich deren Software für nicht sicher halte ist dabei gar nicht das Argument, ich finde es grundsätzlich falsch Schülerdaten irgendwelchen Firmen in die Hand zu geben.

Randnotiz:
In manchen Bundesländern gibt es eine "amtliche" Schulverwaltungs-Software, bei der auch Noten "bequem" webbasiert via Smartphone etc. vom Fachlehrer eingetragen werden können,
Wie sicher diese Software ist, wird sich (leider) noch zeigen. Der bisherige track record von Bund und Ländern, was digitale "Projekte" angeht, ist katastrophal: De-Mail, elektronische Gesundheitskarte, Modesta, JobCard/Elena, PC-Wahl, beA, ella, und wie sie alle heißen.

Beitrag von „plattyplus“ vom 19. Juni 2018 18:32

> Zitat von Morse
>
> In manchen Bundesländern gibt es eine "amtliche" Schulverwaltungs-Software, bei der auch Noten "bequem" webbasiert via Smartphone etc. vom Fachlehrer eingetragen werden können

Diese Software gibt es bei uns in NRW auch, nennt sich "SchilD".

Problem dabei: Die Software ist dermaßen buggy und mit irgendwelchen Funktionen überladen, die hier und da immer weiter an die Datenbank drangebaut wurden, daß man die Software kaum bedienen kann. Das fängt schon damit an, daß die Namen nach schwedischem Alphabet sortiert werden (Umlaute sind ganz hinten im Alphabet), wohl weil die Entwickler beim ersten Wurf der Software in den 1980ern eine schwedische Tastaturbelegung oder so eingestellt hatten. Weiter geht es mit einer falschen Berechnung der zusammengesetzten Abschlußnoten usw. usw. ...

Außerdem haben wir mit der Software massive Probleme, weil sie unser Virenscanner regelmäßig als Virus erkennt und in die Quarantäne schickt oder gleich löscht. 

Beitrag von „O. Meier“ vom 19. Juni 2018 20:56

> Zitat von Morse
>
> RPs, die zentrale Datenschutz-Beauftragte einzelnen Schulen zuordnen, weil sich dort niemand mehr findet, der diesen Job machen will

Es müsste sich erstmal jemand finden, der den Job machen *kann*. Dazu braucht man nicht unerhebliche juristische und technische Kenntnisse. Auf dem Posten sind die Kollegen, die sich dazu breit schlagen lassen, nur Feigenblätter.

> Zitat von Morse
>
> Projekte" angeht, ist katastrophal: De-Mail, elektronische Gesundheitskarte, Modesta, JobCard/Elena, PC-Wahl, beA, ella, und wie sie alle heißen.

Toll Collect (läuft zwar mittlerweile, ging aber mit arger Verspätung an den Start. Danach wurde sich jahrelang um die Abeechung gestritten), elektronisches Anwaltspostfach (hattest du wohl schon), Logineo ...

Beitrag von „Valerianus“ vom 20. Juni 2018 06:44

Ich hab ehrlich gesagt lieber einen kommerziellen Anbieter, bei dem ich genau nachvollziehen kann was passiert (keinerlei Internetverbindung ist für mich das wichtigste Sicherheitsmerkmal), weil er ansonsten finanziell ruiniert ist, als dass die öffentliche Hand irgendetwas programmiert, bei dem man hinten und vorne den fehlenden Sachverstand bemerkt...

Beitrag von „Morse“ vom 20. Juni 2018 11:13

> Zitat von Valerianus
>
> Ich hab ehrlich gesagt lieber einen kommerziellen Anbieter, bei dem ich genau nachvollziehen kann was passiert (keinerlei Internetverbindung ist für mich das wichtigste Sicherheitsmerkmal), weil er ansonsten finanziell ruiniert ist, als dass die öffentliche Hand irgendetwas programmiert, bei dem man hinten und vorne den fehlenden Sachverstand bemerkt...

Wie kannst Du bei einem kommerziellen Anbieter "genau nachvollziehen was passiert"? Der Code ist Betriebsgeheimnis.

Teilweise ist ja ganz überraschend, was da ans Licht kommt, wenn z.B. schon ein Programm wie MS Word sich mit 15 verschiedenen Außenstellen in Verbindung setzt, ohne, dass der User davon etwas mitbekommt.

Beitrag von „Valerianus“ vom 20. Juni 2018 15:19

Und der Code bei öffentlich-rechtlichen Programmen ist Open Source? 
Natürlich kann ich nachvollziehen ob ein Programm Daten ins Internet rausschickt. Wie gesagt: Wenn ein Programm die Klappe hält, ist mir das erst einmal Sicherheitsfeature genug und die korrekte Implementierung von Verschlüsselung ist üblicherweise auch keine Raketentechnik, das kriegen die schon hin. 

Beitrag von „Krabappel“ vom 20. Juni 2018 15:33

> Zitat von Elmorya
>
> ...
> Ich bin diesbezüglich etwas perplex, da es m.E. einfacher ist einen Notenkalender zu klauen, als ein Handy zu hacken. Oder irre ich da so sehr?

Ich denke, dass der ganze Digitalekram eine Unübersichtlichkeit nach sich zieht, die kaum noch einer überblicken kann. Wenn dein Notenbuch weg ist, kriegst du's wenigstens mit... (im Übrigen dürfen wir aus diesem Grund auch keine privaten Notenbücher haben.)

Früher hat man auch auf Klassenfahrten fotografiert, hinterher Nummern aufgeschrieben "...schrill! da bin ich drauf, wie ich Chips esse! das Bild will ich!" und nachbestellt. Heute kann gleich jedes Desaster online gestellt werden und auf ewig jede Einstellungschance bei künftigen Arbeitgebern versauen...

Und noch was: Noten sind das eine. Fehltage, Angaben zu Elterngesprächen etc. weitere private Daten. Ich möchte sowas von meinen Kindern auch nicht online wissen, am besten mit dem Passwort "lehrer" geschützt.

Beitrag von „Valerianus“ vom 20. Juni 2018 16:52

Ich glaube, dass wir hier zwischen cloudbasierten Lösungen und fest installierten Lösungen unterscheiden müssen. Die Häufigkeit mit der manche Kollegen OneNote365 oder Dropbox nutzen macht mich auch immer wieder sprachlos...

Beitrag von „plattyplus“ vom 20. Juni 2018 21:06

> Zitat von Valerianus
>
> Ich glaube, dass wir hier zwischen cloudbasierten Lösungen und fest installierten Lösungen unterscheiden müssen.

Wobei die Grenzen da aber auch fließend sind. Bei uns an der Schule können z.B. per Remote Desktop Verbindung (rdp) sich alle Kollegen von zuhause aus auf dem Schulserver einloggen und dort SchilD öffnen und Schülerdaten bearbeiten. Da hängt dann auch die eigentlich lokale Software auf einmal voll im Internet.

Beitrag von „Morse“ vom 21. Juni 2018 00:10

> Zitat von Valerianus

> Und der Code bei öffentlich-rechtlichen Programmen ist Open Source? 
> Natürlich kann ich nachvollziehen ob ein Programm Daten ins Internet rausschickt. Wie gesagt: Wenn ein Programm die Klappe hält, ist mir das erst einmal Sicherheitsfeature genug und die korrekte Implementierung von Verschlüsselung ist üblicherweise auch keine Raketentechnik, das kriegen die schon hin. 

Die genannten staatlichen Programme sind nicht Open Source, aber da trägt dann auch das Land die Verantwortung.

"Wenn ein Programm die Klappe hält, ist mir das erst einmal Sicherheitsfeature genug"
Ob ein Programm "die Klappe hält", oder nicht, merkt ein User gar nicht.

Die Einstellung "das kriegen die schon hin" finde ich naiv. Ich kann nicht nachvollziehen, worauf sich dieses blinde Vertrauen gründet. Es gab doch schon zig "Datenpannen", die Schlagzeilen gemacht haben.

Beitrag von „Valerianus“ vom 21. Juni 2018 06:38

Ob ein Programm "die Klappe hält" merkt ein User, der seinen PC und seine sonstige Hardware unter Kontrolle hat sehr schnell. Ich kann dir, wenn ich das möchte die genauen Zeiten sagen, wann welches Programm Zugriff aufs Internet hatte (und das ist seit ein paar Jahren kein schöner Anblick mehr, weil andauernd irgendein Programm irgendwas aus dem Internet will...Windows braucht dringend ein zentrales Update-System für alle installierten Programme...)

@plattyplus: Das ist ja quasi der datenschutztechnische Super-GAU. Läuft das getunnelt und wie stellt euer Admin die Integrität der einzelnen zugreifenden Systeme fest?

Beitrag von „Morse“ vom 21. Juni 2018 10:11

> Zitat von Valerianus
>
> **Ob ein Programm "die Klappe hält" merkt ein User, der seinen PC und seine sonstige Hardware unter Kontrolle hat sehr schnell.** Ich kann dir, wenn ich das

> möchte die genauen Zeiten sagen, wann welches Programm Zugriff aufs Internet hatte (und das ist seit ein paar Jahren kein schöner Anblick mehr, weil andauernd irgendein Programm irgendwas aus dem Internet will...Windows braucht dringend ein zentrales Update-System für alle installierten Programme...)

"Ein User, *DER*", da hast Du schon recht, aber wenn Du im Kollegium fragst, wer Netzwerk Monitoring macht, werden die allmeisten wohl zurückfragen, was das überhaupt sein soll.
Insofern scheint es mir schon so zu sein, dass 99,99% der User nicht mitbekommen, wenn Software nachhause telefoniert.
Davon abgesehen hast Du ja die Verschlüsselung angesprochen: auch wenn protokollierst, welche Prozesse Daten senden, weißt Du nicht welche Daten.
Sag jetzt nicht, dass "ein User, der seinen PC und seine sonstige Hardware unter Kontrolle hat" Verschlüsselung sehr schnell knacken kann!

Beitrag von „Valerianus“ vom 21. Juni 2018 15:14

Bei der Verschlüsselung geht es mir eher um die Sicherheit der Implementierung, d.h. darum dass jemand außer mir die nicht mit zumutbarem Aufwand knacken kann. Ich hab nicht die Rechenleistung zuhause rumstehen, um das hinzubekommen. Ich halte nur den Rückschluss "öffentliche Verwaltung" = sichere Software für extrem trügerisch. Was die Haftungsfrage angeht hast du natürlich Recht, da ist man fein raus, wenn der Dienstherr einem Software stellt.

Beitrag von „Morse“ vom 22. Juni 2018 00:06

> Zitat von Valerianus
>
> Ich halte nur den Rückschluss "öffentliche Verwaltung" = sichere Software für extrem trügerisch.

Den Rückschluß machte ich ja nicht, ganz im Gegenteil (siehe Beitrag 35) - insofern stimme ich Dir da absolut zu!

Beitrag von „Morse“ vom 20. September 2018 18:15

> Zitat von O. Meier
>
> Toll Collect (läuft zwar mittlerweile, ging aber mit arger Verspätung an den Start. Danach wurde sich jahrelang um die Abeechung gestritten), elektronisches Anwaltspostfach (hattest du wohl schon), Logineo ...

Neues von der Digitalisierung in B.-W.:

"**Digitale Bildungsplattform für Schulen**
„ella“ verzögert sich wohl um mehrere Jahre":
https://www.stuttgarter-zeitung.de/inhalt.digital...f6d448743e.html