# „Der Schlüssel muss vorhanden sein“

## Interview mit Holger Engelland, der seit 19 Jahren Daten rettet

***Cloud Computing erhöht das Risiko von Datenverlusten. Logisch oder physikalisch beschädigte Daten von allen Speichermedien und Betriebssystemen werden beim Böblinger Unternehmen Kroll Ontrack in weltweit 20 Laboren und Reinräumen mit eigens entwickelten Werkzeugen wieder verfügbar gemacht. Verschlüsselung ist in. Sind die Böblinger auch ein Schlüsseldienst?***

***OBJEKTspektrum: Herr Engelland, dem Branchenverband BITKOM zufolge, verschlüsseln mehr als drei Viertel aller deutschen Unternehmen ihre Mails und Daten. Auf welche Verschlüsselungsmethoden stoßen Sie, wenn Sie als Datenretter zu Hilfe geholt werden?***
*Holger Engelland: Auf alle. Derzeit sind rund zwei Dutzend verschiedene Verschlüsselungsmethoden auf dem Markt. Neben den Verschlüsselungsalgorithmen muss man zwischen hard- und softwareseitiger Verschlüsselung unterscheiden. Egal, ob es sich um eine ältere oder neuere Methode handelt, irgendwann landet faktisch jede Verschlüsselung in Form eines defekten oder von Datenverlust betroffenen Speichermediums bei uns im Datenrettungslabor.*

***Was ist die Mindestvoraussetzung dafür, dass Sie verschlüsselte Daten wiederherstellen können?***
*Der Schlüssel muss vorhanden sein. Ansonsten ist es selbst für Datenretter mit den heutzutage verfügbaren Bitschlüssellängen nicht möglich, auf die Festplatte oder den Flash-Speicher zuzugreifen.*

***Was sollten Unternehmen bei Verschlüsselungen demgemäß beachten?***
*Wenn sie die Wahl haben, sollten sie sich immer für eine Software-Verschlüsselung mit der Wahl eines eigenen Schlüssels entscheiden. Diese verursacht bei einer Datenwiederherstellung deutlich weniger Probleme als eine herstellerdefinierte Hardware-Verschlüsselung. Oftmals geben die Produzenten ihren Masterschlüssel bei einem Datenverlust nicht heraus und verhindern so eine erfolgreiche Datenrettung. Bei einer Datenrettung von einem verschlüsselten Speicherträger sollte der Schlüssel also immer dem Datenrettungsspezialisten mitgeliefert werden.*

***Stellen ältere Verschlüsselungsverfahren ein besonderes Problem für die Datenrettung dar, weil man besonders schwer an die Schlüssel zum „Aufsperren“ herankommt? Sollte man die verwendeten Verfahren von Zeit zu Zeit erneuern?***

Foto: Kroll Ontrack

Datenverlust ist schmerzhaft. Für manche ist er der rettende Engel: Holger Engelland (49) ist als „Manager Data Recovery Engineering“ Leiter des Datenrettungslabors bei Kroll Ontrack.

*Es ist eher so, dass man bei den älteren Verschlüsselungsverfahren noch eine minimale Chance hat, die Verschlüsselung zu umgehen. Aber meistens spielt das Alter keine Rolle. Aus unserer Sicht sollte man bei Unternehmen und Behörden in den Datenmanagement-Verfahren die Sicherstellung der Funktionsfähigkeit einer End-to-End-Verschlüsselung implementieren, damit es nicht zu unerwarteten Situationen kommt.*

***Sind hardwareseitig verschlüsselte Flash-Laufwerke, also Self-Encrypting-Drives, zu empfehlen?***
*Aus Sicht der Datenrettung, nein.*

***Wie lassen sich speziell bei Hardware-Verschlüsselung Probleme vermeiden?***
*Mit der Verschlüsselung an sich gibt es aus unserer Sicht keine Probleme – die Probleme fangen erst an, wenn der passende Schlüssel verschwindet.*

***Braucht man für Software-Verschlüsselung einen extra Verschlüsselungsbeauftragten im Unternehmen?***
*Nein, es reicht, wenn sich die für den Datenschutz und das Datenmanagement zuständigen Mitarbeiter über die Funktionalität der Datenverschlüsselung im Rahmen der geltenden Prozesse abstimmen.*

***Wo sollte man Softwareschlüssel am besten lagern?***
*An einem sicheren Ort und auf einem anderen – möglichst neuwertigen – Speicherträger.*

***Sollte man Ihrer Meinung nach auch im privaten Umfeld Verschlüsselung einsetzen?***
*Das kommt darauf an, worüber wir hierbei reden. Wenn es sich um private E-Mail-Kommunikation handelt und man nicht möchte, dass auf die Inhalte zugriffen werden kann, dann würde ich persönlich eine Verschlüsselung, beispielsweise PGP, anwenden. Man muss sich darüber im Klaren sein, dass es sich bei E-Mails um eine Kommunikationsform handelt, bei der, wie bei einer Postkarte, andere sehr leicht mitlesen können. Allerdings empfiehlt es sich, eine Verschlüsselung nur bei wirklich sensitiven Informationen einzusetzen. Bei Speichermedien würde ich im privaten Umfeld auf eine Verschlüsselung verzichten und stattdessen lieber die externe Festplatte – USB-Stick oder DVD – in einen Tresor einschließen. Die Gefahr, die Verschlüsselung zu verlieren und damit zu riskieren, dass bei einem Defekt nicht einmal professionelle Datenretter auf mein Medium zugreifen können, wäre zu hoch.*

***Welche Verschlüsselungsmethoden würden Sie Bundestagsabgeordneten für deren Kommunikation empfehlen?***
*Genau die gleichen, die ich auch Normalbürgern vorschlagen würde: Wenn überhaupt, dann eine sichere. Also eine Verschlüs-*

*selung möglichst mit einer 128-Bit- oder höheren Schlüssellänge. Diesen Schlüssel mit einem Supercomputer zu berechnen, würde wahrscheinlich länger als das angenommene Alter unseres Universums dauern. 256-Bit Verschlüsselungen sind nach menschlichem Ermessen gar nicht zu knacken. Wer also seine Festplatte so verschlüsselt und die Schlüssel später verliert – sei es physisch oder weil das Medium unwiederbringlich kaputt gegangen ist – kann seine Hoffnung auf eine Wiederherstellung der gespeicherten Daten für immer vergessen. Darüber muss man sich im Klaren sein.*

*Das Interview führte Annegret Handel-Kempf.*

# „Private Inhalte sollen wieder im Internet geteilt werden können"

## Interview mit Nils Kenneweg, Gründer des Berliner Startups whispeer

***Der Trend ist klar: Längst wollen die Nutzer sozialer Netzwerke nicht mehr jeden in ihren Mitteilungsbereich hereinlassen. Doch auch in der Online-Kommunikation müssen Verschlüsselung und Entschlüsselung reibungslos funktionieren, damit der Frust mit den Schlüsseln nicht am Ende noch Freundschaften zerstört. OBJEKTspektrum fragte beim Berliner Startup whispeer nach, das sich der Mission „einfache, private Online-Kommunikation im Internet" verschrieben hat.***

***OBJEKTspektrum: Wie lässt sich der Kreis derer, die meine Nachrichten lesen, einschränken?***

*Nils Kenneweg: Der Dreh- und Angelpunkt bei whispeer ist das Passwort des Nutzers. Dieses sollte stark und lang sein, um eine gute Verschlüsselung zu gewährleisten. Weiterhin ist der Account nicht mehr erreichbar, wenn man das Passwort und den Backup-Key verliert. Wenn eine Nachricht auf whispeer versendet wird, so ist diese automatisch nur von den gewählten Empfängern lesbar. Wir setzen nicht darauf, die Reichweite von Inhalten einzuschränken, sondern darauf, dass Leser explizit freigegeben werden müssen.*

***Sie sind Hauptentwickler von whispeer. Wie sind Sie und Ihre Mitstreiter Daniel Melchior, Michelle Thenhausen und Martin Czuchra vor vier Jahren auf die Idee gekommen, die Nutzer sozialer Netzwerke wie Facebook oder Twitter, die doch eher öffentlichkeitsorientiert sind, mit Privatheit zu versorgen?***
*Die Idee kam uns, als uns klar wurde, dass private Inhalte im Internet nicht privat sind, was mittlerweile vielfach bestätigt wurde. Heutzutage ist jedem bewusst, dass selbst eine „private" Nachricht auf Facebook nicht vollständig privat ist. Dies hat dazu geführt, dass private Inhalte immer weniger im Internet geteilt werden, was wir durch whispeer wieder ermöglichen möchten. Wir sprechen aber nicht nur Facebook- oder Twitter-Nutzer an, sondern insbesondere auch Nutzer, die nicht bei besagten Diensten sind, gerade weil die Privatsphäre bei diesen Diensten nicht gegeben ist.*

***Jedes Zeichen wird noch auf der Sender-Seite unlesbar gemacht und erst auf der Empfänger-Seite wieder zurück verwandelt?***
*whispeer arbeitet mit asymmetrischen und symmetrischen Schlüsseln, um die Daten der Nutzer zu verschlüsseln. Hierbei verwenden wir AES[1]) und elliptische Kurven. Jegliche Verschlüsselung findet auf dem Rechner des Nutzers statt und Daten können nur vom Nutzer und vom ausgewählten Empfänger entschlüsselt werden. Schon bei der Registrierung wird ein asymmetrisches Schlüsselpaar erzeugt, das aus einem öffentlichen und einem privaten Schlüssel besteht. Der öffentliche Schlüssel wird auf dem whispeer-Server hinterlegt. Der private Schlüssel wird mit dem Passwort verschlüsselt auf dem Server abgelegt, um ein einfaches Einloggen auf einem neuen Gerät zu ermöglichen. Das Passwort wird nicht an den Server übertragen. Will Nutzer Alice nun mit Nutzer Bob kommunizieren, so holt Alice zuerst Bobs öffentlichen Schlüssel vom Server und verwendet diesen, um einen symmetrischen Zwischenschlüssel zu erzeugen, der nur von Bob entschlüsselt werden kann. Mit diesem verschlüsselt Alice nun die Nachricht. Die verschlüsselte Nachricht wird dann auf dem Server abgelegt und von Bob später abgerufen und mit seinem privaten Schlüssel entschlüsselt. Der Server hat weder Zugriff auf Bobs privaten Schlüssel, den Nachrichtenschlüssel, noch auf Bobs Passwort.*

***Die Quelltexte Ihrer Web-App sind auf Github veröffentlicht, aber nicht unter einer Open-Source-Lizenz. Warum?***
*Wir sind der Überzeugung, dass Sicherheit nur möglich ist, wenn die Quelltexte für die Öffentlichkeit zugänglich und überprüfbar sind. Hierfür ist eine Open-Source-Lizenz aber nicht notwendig.*

Foto: whispeer

Daniel Melchior (links) und Nils Kenneweg (23), der IT-Systems Engineering im Mastergang studiert, tüfteln seit vier Jahren daran, Privatsphäre im Netz sicherer zu machen: Weil es für die beiden ganz normal ist, online auch mal wichtige Dinge zu besprechen, entwickelten sie mit Freunden ein Netzwerk, in dem einfach und sorglos, aber sicher ohne unerwünschte Mitleser kommuniziert werden soll.

[1]) *Anm. d. Red.: „Advanced Encryption Standard" gilt als eine besonders sichere Blockchiffre.*

*Da whispeer noch eine junge Firma ist, wollen wir uns bezüglich der Lizenz alle Optionen offenhalten.*

***Die Grundfunktionen von whispeer sollen kostenlos bleiben. Noch finanzieren Sie und Ihre Kollegen das Projekt. Wie soll sich der Dienst auf Dauer rechnen?***
*Kurzfristig planen wir, durch Spenden Einnahmen zu generieren. Mittelfristig setzen wir auf kostenpflichtige Zusatzfunktionen und langfristig planen wir einen Großteil der Einnahmen über Firmenkunden zu generieren, die ihre interne und externe Kommunikation absichern wollen.*

***Welche kostenpflichtigen Zusatzfunktionen könnten Sie sich vorstellen, die im Sinne Ihrer Website-Versprechen keine „extra Funktionen, keine verwirrenden Optionen" sind?***
*Wir stellen uns zum Beispiel den Versand großer Dateien und das Teilen hochauflösender Bilder als kostenpflichtige Zusatzfunktionen vor. Wir werden aber auf Nutzerwünsche eingehen und unsere Strategie diesbezüglich anpassen.*

***Wie könnten Firmen whispeer in ihre Unternehmenskommunikation integrieren?***
*Unternehmen können schon heute whispeer in der kostenlosen Version ausprobieren und hiermit eine einfache und sichere Kommunikation benutzen. Whispeer bietet für Firmen zusätzlich einen sicheren und einfachen Dateiversand, mit dem sowohl interne als auch externe Personen erreicht werden können, was insbesondere bei externen Personen einen hohen Sicherheitsvorteil bietet. Weiterhin bietet whispeer eine einfache Kommunikation in Gruppen. Whispeer ist insbesondere nützlich, wenn Mitarbeiter nicht vor Ort sind, sondern z. B. auf Messen oder im Feld, da whispeer durch die Verschlüsselung und die Benutzbarkeit auf vielen Geräten eine Kommunikation auch aus dem Feld ermöglicht. Aus diesem Grund wurde auch eine App entwickelt, die aktuell in einer geschlossenen Beta-Phase getestet wird.*

***Ihr Startup kostete Sie bereits viele hundert Stunden unbezahlter Arbeit. Bleibt Ihnen noch Zeit für Ihre Freunde, auch jenseits sozialer Netzwerke?***
*whispeer nimmt viel Zeit in Anspruch. Wir glauben aber an die Mission und sind bereit, diese Zeit zu investieren. Die Zeit für Freunde ist durch whispeer weniger geworden, aber trotzdem natürlich noch vorhanden.*

***Wie sollen an Privatheit interessierte Menschen whispeer mit freiwilligen Spenden unterstützen, wenn Ihre Kontaktdaten anscheinend nur über Facebook zu finden sind?***
*Die Kontaktdaten sind auch auf der whispeer Startseite verfügbar, z. B. im Impressum. Wenn man einfach spenden möchte, kann man sich auch einen Account erstellen und nach dem Einloggen auf den Menüpunkt „Unterstütze whispeer" klicken.*

*Das Interview führte Annegret Handel-Kempf.*