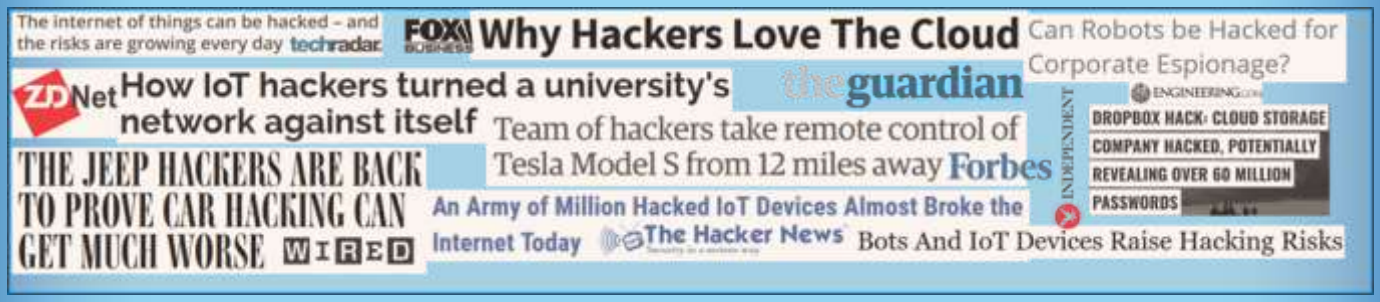
LUCKYSTOR Cyber Secure Cloud Storage
Disruptive völlig neue IKT Sicherheit



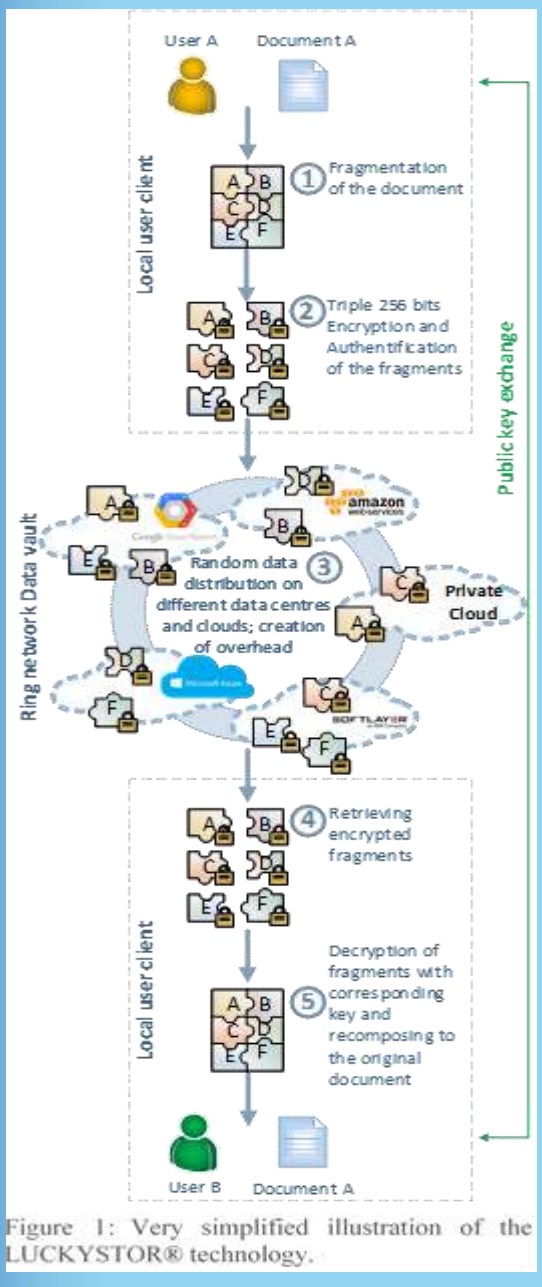


Figure 1: Very simplified illustration of the LUCKYSTOR® technology.

LUCKYSTOR® ist eine offene, plattformunabhängige und dezentrale Cloud-basierte Speichertechnologie, die nonSQL Data Bases und Dateien "end-to-end" verschlüsselt und sicher über Internet und Intranet überträgt, um die Privatsphäre der Nutzer zu schützen. Auf der Basis der LUCKYSTOR®-Technologie können Unternehmen und Privatanwender einen sicheren Cloud-Speicher implementieren, der ohne zentrale Server verwaltet werden kann und damit das ultimative Ziel "kein einziger Angriffspunkt" erreicht. Die LUCKYSTOR®-Technologie arbeitet wie in Abbildung 1 dargestellt und wird im folgenden Absatz beschrieben.

Daten, die der Benutzer sicher übertragen möchte, werden von der LUCKYSTOR® Client Software in Datenblöcke (Slicing) zerlegt. Gleichzeitig wird ein Schlüsselpaar für die End-to-End-Verschlüsselung erzeugt. Die Datenblöcke werden dann mit drei verschiedenen Verschlüsselungsmethoden verschlüsselt (Diffie Hellmann elyptische Kurve, David Bernstein NaCl Bibliothek, Salsa 20). Dabei werden die Datenblöcke weiter fragmentiert. Im nächsten Schritt werden die verschlüsselten Fragmente zufällig von einem dynamischen Algorithmus an mehrere virtuelle Serverknoten in verschiedenen Rechenzentren verteilt, die sich in Europa, den USA oder irgendwo sonst auf der Welt befinden - ohne zentrale Instanz (Ringnetz). Diese Rechenzentren können öffentliche Cloud-Anbieter sein (z. B. Amazon Web Services, Google Cloud Platform, Microsoft Azure, IBM Softlayer, Host Europe, Strato, 1&1,…), aber auch private Clouds in einem Firmennetzwerk oder Hybrid-Clouds, die bestimmte

T&T CloudCrowding Solutions GmbH · Kochstraße 19 · 74405 Gaildorf
07971 / 919 30 39 · info@cloudcrowding.de
www.cloudcrowding.de

Elemente von öffentlichen Cloud-Providern in die eigene Private Cloud integrieren. Automatisch generierte Metadaten und Etiketten stellen sicher, dass die Fragmente später gefunden und auf das Originaldokument wiederhergestellt werden können. Durch die Verteilung der Fragmente an mehrere Server und Rechenzentren hat kein Administrator oder Hacker Zugriff auf alle Daten, und selbst wenn einer der drei Verschlüsselungsalgorithmen kompromittiert wurde, hat der Administrator / Hacker noch keine Möglichkeit, die Datei zu lesen. Dabei wird ein Overhead von 130% der Daten durch statistische Spiegelung erzeugt. Der Zweck dieses Overhead ist es, eine hohe Verfügbarkeit der Fragmente und ein laufendes Disaster Recovery zu gewährleisten. Die Verwendung einer RESTful API ermöglicht die Verarbeitung von sowohl strukturierten als auch unstrukturierten Daten und insbesondere die Übertragung und Speicherung ganzer Dateisysteme. Bei der Kommunikation / Datenübertragung kann ein anderer autorisierter Benutzer die Fragmente von den Servern herunterladen oder empfangen. Mit der entsprechenden Funktion kann der Benutzer das Dokument verschlüsseln. Dieser Vorgang funktioniert genauso wie die Datenspeicherung eines einzelnen Benutzers anstelle der Kommunikation / Datenübertragung.

Das LUCKYSTOR®-Konzept basiert auf einem Geheimteilprinzip von Massachusetts Institute of Technology. Die Idee ist, Geheime Informationen zu fragmentieren und jedem einzelnen Fragment einen eigenen, einzigartigen Teil des Geheimnisses zu geben. Die Daten und Informationen können nur rekonstruiert und gelesen werden, wenn alle Teile vereint sind. In LUCKYSTOR® kennt nur der Benutzer den verwendeten Algorithmus und kann die Fragmente zusammenstellen, um das Originaldokument wiederherzustellen.

Bei konventionellen Systemen stellt die Firewall oft nur den Schutz für die sensiblen Daten von außen dar. Cyber-Kriminelle dringen immer mehr durch und haben vollen Zugriff auf alle Daten und manchmal sogar auf zusätzliche Computer / Server im Netzwerk, sobald sie die Firewall gehackt haben. Mit LUCKYSTOR® können Hacker und Administratoren jedoch die fragmentierten und verschlüsselten Daten nicht nutzen, auch wenn sie die Firewall überwinden und in das System gelangen (siehe Abbildung 4):

• Daten stehlen und / oder lesen:

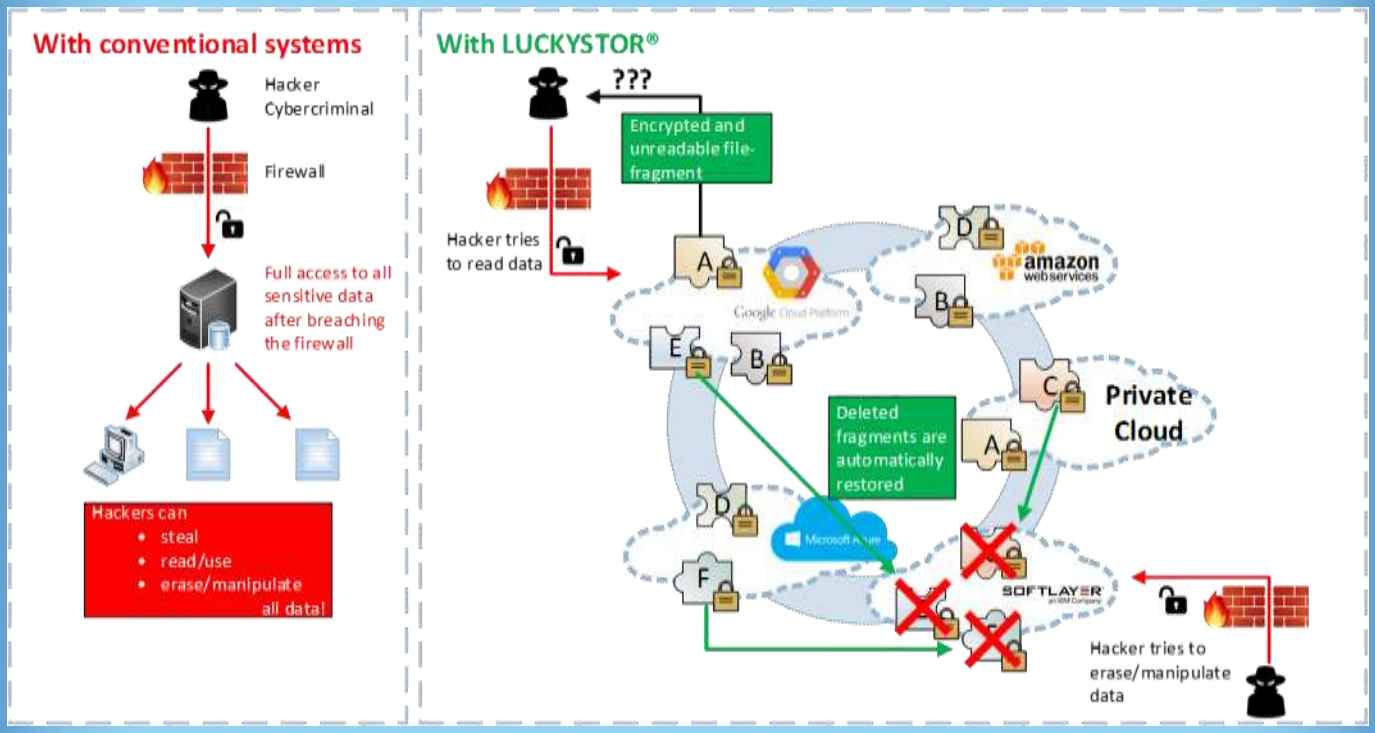
Nach dem überwinden der Firewall können Hacker nur verschlüsselte und nicht zusammenhängende Dateifragmente sehen. Auch wenn sie es schaffen sollten, die Verschlüsselung zu brechen, liefern die Datei-Fragmente immer noch keine wertvollen Informationen. Es ist ihnen unmöglich, alle relevanten Fragmente zu finden und sie zu einem kompletten Dokument zu kombinieren, da sie weder die anderen Server noch die Verteilung der Fragmente kennen, noch können sie die 3 Verschlüsselungstechnologien entschlüsseln.

• Daten löschen oder manipulieren:

Wenn der Hacker versucht, die Datei-Fragmente auf dem Server zu löschen oder zu manipulieren (z.B. nach einem fehlgeschlagenen Versuch, die Dokumente zu lesen), bemerken die LUCKYSTOR®-Algorithmen (Monitoring) die Änderung und stellen automatisch die gelöschten / kompromittierten Dateifragmente aus dem erzeugten Overhead wieder her. Ein ständiges Desaster Recovery ist verfügbar.

- Server antwortet nicht:

Wenn entweder durch einen Angriff oder einen technischen Ausfall ein ganzer Server (oder sogar Cloud Service) offline ist, kann LUCKYSTOR® die fehlenden Dateifragmente im Verteilungsnetzwerk neu zu ordnen und die vollständige Datenverfügbarkeit wiederherstellen. Wenn mindestens 60-70% der Daten verfügbar sind, kann LUCKYSTOR® die gesamten Dateien wiederherstellen. Mit dieser Funktionalität sind auch Datenumzügen leicht realisierbar.



- **Weitere Vorteile:**
- **Signifikante Steigerung der Zuverlässigkeit und Verfügbarkeit**
- **Signifikante Steigerung der aktiven Informationssicherheit**
- **Signifikante Verbesserung der Datenintegrität (Ownership)**
- **Signifikante Reduzierung von Kosten (Cent/GB)**
- **Signifikante Steigerung von Speed und Performance**
- **Signifikante Vereinfachung von Operations und Administration**
- **Signifikante Steigerung der Skalierbarkeit**
- **Vollständiges Desaster Recovery**
- **Hohe digitale Souveränität**
- **Signifikante Steigerung der Produktsicherheit**