Vision Statement

SecureDoc™ by WinMagic

WinMagic – unsere Vision für eine bessere Datensicherheit in einer komplexen Welt

AUGUST 2019

WINMAGIC®

Seit über 21 Jahren genießt WinMagic seinen wohlverdienten Ruf als Vordenker und Innovator im Bereich Datenverschlüsselung. Im Laufe der Jahre haben wir in der Branche viel Pionierarbeit geleistet. So konnten wir dazu beitragen, die Messlatte für Sicherheit und Verwaltbarkeit für Unternehmen in aller Welt höher zu legen. Mit Blick auf die Zukunft ist es unser Ziel, außerordentlich leistungsstarke und **intelligente Lösungen rund um die Verschlüsselung** anzubieten und die Sicherheit auch in komplexen Umgebungen zu vereinfachen.

Die Vision von WinMagic – der einfache Weg zur Optimierung der Datensicherheit

Da die Datensicherheit in der modernen digitalen Welt für Unternehmen eine zunehmend wichtige Rolle spielt, ist WinMagic der Meinung, dass eine wichtige Frage zu diesem Thema bereits beantwortet wurde. Unsere Vision konzentriert sich auf drei Punkte:

1. **Die Kryptografie** (bei der die Verschlüsselung ein wichtiger Bestandteil ist) **sollte künftig die** Grundlage für Daten und die IT-Sicherheit sein.
2. **Eine effiziente Datensicherheit beginnt mit sicheren Workloads**. Sobald alle Endpunkte geschützt sind, wird es für Angreifer sehr schwierig, sich Zugriff auf kritische Daten zu verschaffen – selbst in der Cloud. Die meisten Sicherheitsstrategien konzentrieren sich jedoch weiterhin auf Server und vernachlässigen Schwachstellen an Endpunkten. Der Ansatz von WinMagic ist einzigartig und schließt eine bedeutende Lücke im modernen Sicherheitsmarkt. Indem wir uns auf den Schutz von Endpunkten konzentrieren, helfen wir bei der Erweiterung, Verbesserung und Integration der Datensicherheit im gesamten Unternehmen.
3. **Verschlüsselung und Schlüsselverwaltung sollten plattformübergreifend sein**. Ein Vorreiter im Bereich Datensicherheit muss her, um plattformunabhängige Lösungen bereitzustellen, die für alle funktionieren.

Herausforderungen und Möglichkeiten im Bereich Datensicherheit

Neue Technologien wie die Cloud und andere Innovationen vergrößern die Angriffsfläche, sodass Daten anfällig für immer neue und größere Bedrohungen werden. Um diese Bedrohungen zu bekämpfen, werden laufend weitere Technologien eingeführt – von der künstlichen Intelligenz (KI) bis hin zu Big Data. Aber dieses „Wettrüsten“ spielt den Angreifern in die Karten. Die Folge: Es gibt immer mehr Sicherheitsanbieter und Lösungen am Markt, ohne dass Daten auf der grundlegenden Ebene geschützt werden. Das ist ein kurzfristiger Gewinn mit langwierigen Problemen.

WinMagic konzentriert sich auf die Kryptografie. Bei ordnungsgemäßer Anwendung verhindert sie Angriffe von außen, indem die Angriffsfläche deutlich verkleinert und so das Vertrauen in die Datensicherheit wiederhergestellt wird. Diese kleinere Angriffsfläche vereinfacht und verbessert den Schutz, benötigt weniger Lösungen und bietet mehr Sicherheit gegen die ständig wachsende Zahl von Bedrohungen.

a. **Die meisten Verschlüsselungslösungen sind wenig ausgereift.** Stellen wir uns einige grundlegende und offensichtliche Fragen: Wann und wo sollten vertrauliche Daten verschlüsselt werden? Welche Art von Verschlüsselungs-Key sollte eingesetzt werden? Wer sollte beispielsweise Zugriff auf den Key haben und damit auf Klartextdaten zugreifen können? Im Idealfall sollten sensible Daten immer verschlüsselt werden, wenn sie nicht gerade verarbeitet werden, z. B. von einer Anwendung, die Daten im Klartext benötigt. Nur entsprechend berechtigte Benutzer sollten den Verschlüsselungs-Key dieser Daten besitzen. Der Großteil der aktuellen Lösungen ist jedoch nicht so ausgereift. Netzwerkgeräte verschlüsseln Daten möglicherweise nicht, bevor sie den Endpunkt verlassen. Hinzu kommt, dass Daten mit Keys verschlüsselt werden, die der Appliance, dem Administrator oder sogar den Dienstanbietern zur Verfügung stehen. Die meisten heute gängigen Angebote – darunter auch Cloud Access Security Broker (CASB)– lassen sich zwar einfach implementieren, aber es gibt durchaus bessere Lösungen!

b. **Integrierte Verschlüsselung ist der De-facto-Standard.** Im Gegensatz zu den Anfangszeiten von WinMagic integrieren die heutigen Plattformanbieter die Verschlüsselung meist in ihre Betriebssystem- oder Plattformumgebungen. Verschlüsselungslösungen wie BitLocker für Windows, dm-crypt für Linux und FileVault 2 für Mac sind ebenso beliebt wie die integrierte Verschlüsselung von AWS und VMWare. Da sie sich jedoch nicht auf die Verschlüsselung

konzentrieren, bieten Plattformanbieter – wenn überhaupt – nur minimale Schlüsselverwaltungs- und andere Funktionen.

Darüber hinaus erfordern einige Verschlüsselungslösungen, dass der Verschlüsselungs-Key vom Managed Service Provider (MSP) abgerufen werden muss. So entsteht eine inhärente Schwachstelle im System. Nehmen wir z. B. „Bring Your Own Key (BYOK)". Hier benötigt der MSP den Key, um das System betreiben zu können. Jeder Besitzer eines Notebooks geht davon aus, dass der Hersteller keinen Zugriff auf seine Daten hat. Cloud-Unternehmen mussten diesen Kompromiss jedoch eingehen. Sie hatten keine andere Wahl, als den Key zu allen Cloud-Daten weiterzugeben. WinMagic bietet nun eine Alternative. Denken Sie daran, dass sich die Weitergabe von Verschlüsselungs-Keys an Dienstanbieter vom zuvor in Abschnitt a behandelten Problem der Schlüsselverwaltung unterscheidet. In Abschnitt a haben wir uns dem Thema Schlüsselverwaltung gewidmet. Hier geht es um Verschlüsselungsverfahren. Die Verschlüsselung erfolgt durch den MSP, der daher den Key besitzen muss. Das ändert auch keine Schlüsselverwaltungslösung.

c. **Der IT-Sicherheitsmarkt würde von einem Pionier im Bereich Verschlüsselung profitieren.** Dieser Pionier könnte die Kompatibilität des Sicherheitsökosystems zum Nutzen aller Beteiligten – sowohl der Anbieter als auch der Kunden – gewährleisten. Insbesondere benötigt der Markt einheitliche, plattformunabhängige Lösungen, die Daten unabhängig vom Speicherort schützen. Anders ausgedrückt: Man braucht eine universelle Lösung mit voller Interoperabilität zwischen allen Plattformen – vom Internet der Dinge (IoT) über Rechenzentren bis hin zur Cloud. Wir sind der Ansicht, dass WinMagic ideal aufgestellt ist, um künftig im Bereich Verschlüsselung eine solche Vorreiterrolle zu übernehmen.

d. **Die Bedeutung von Virtualisierung und Cloud.** Es ist bekannt, dass Unternehmen der herkömmlichen IT-Infrastruktur den Rücken kehren und zunehmend Virtualisierung und Cloud-Computing nutzen. Wenn der Sicherheitsaspekt geklärt wird, wird sich dieser Trend rasch fortsetzen. Die Sicherheit ist deutlich komplexer geworden, da sich Workloads immer öfter außerhalb des Unternehmens in der Cloud befinden – und somit außerhalb der Kontrolle des Unternehmens. Daten, die zwischen Endpunkt und Cloud, vor Ort in die Cloud oder sogar zwischen den Clouds übertragen werden, benötigen einen umfassenden End-to-End-Schutz.

   Der Fokus von WinMagic liegt schon lange auf der Verlagerung herkömmlicher Endpunkt-Verschlüsselungsverfahren in die Cloud – und somit auf der Revolutionierung der Datensicherheit für die gesamte Branche. Wir verfügen über umfassendes Offline-Wissen und Know-how und möchten das Rad für eine neue Ära der Cloud nicht neu erfinden.

e. **Einhaltung gesetzlicher Vorschriften und Richtlinien**. Die Einhaltung gesetzlicher Vorschriften wie der EU-DSGVO oder HIPAA in den USA und eine leistungsstarke Verschlüsselung sind heute ein Muss für die meisten Unternehmen und Regierungsbehörden. WinMagic ist in der Lage, die erforderlichen Ressourcen bereitzustellen, um politische Entscheidungsträger mit sinnvollen technologischen Lösungen, die sich auf Kryptografie konzentrieren, und anderen Ressourcen zu unterstützen.

Die Bedeutung unserer Vision

Die Grundlage unserer Vision ist unser sogenannter „technologischer" Ansatz – eine klare, fundierte Argumentation, die auf Hightech-Prinzipien basiert.

WinMagic kann eine Schlüsselrolle im internationalen Verschlüsselungsmarkt einnehmen und in naher und ferner Zukunft intelligente Lösungen rund um die Verschlüsselung anbieten.

Die Verschlüsselung besteht aus zwei zentralen Bestandteilen. Die Verschlüsselung und Schlüsselverwaltung müssen voneinander getrennt werden. Während der Plattformanbieter gut aufgestellt ist, um eine leistungsstarke, transparente Verschlüsselungslösung für seine eigene Umgebung zu schaffen, sieht es bei der Schlüsselverwaltung schon ganz anders aus. Eine gute Schlüsselverwaltung muss unabhängig auf vielen verschiedenen Plattformen arbeiten und die Daten des Unternehmens unabhängig vom Speicherort schützen.

Warum ist dies so wichtig?
Da sich die betriebssystemspezifische Verschlüsselung immer weiter ausbreitet, wünschen sich Unternehmen das Beste aus beiden Welten: die Verschlüsselungslösung des Plattformanbieters, die von einer erstklassigen Schlüsselverwaltungslösung verwaltet wird. WinMagic entwickelt auch weiterhin

Lösungen für die Schlüsselverwaltung, die vollständig kompatibel zu BitLocker, FileVault 2, dm-crypt und selbstverschlüsselnden Laufwerken (SEDs) sind – ganz im Gegensatz zu Verschlüsselungskomponenten anderer Anbieter. Unsere Schlüsselverwaltungslösung leistet viel mehr, als nur BitLocker zu verwalten. Sie übernimmt die Pre-Boot-Authentifizierungsfunktion (PBA) und bietet so eine leistungsstarke Schlüsselverwaltung.

Selbstverschlüsselnde Laufwerke (SEDs) – besser als betriebssystemnative Verschlüsselung. Die besten technologischen Innovationen sind intelligent, einfach und effizient. Genau so würden wir SEDs beschreiben. Während die Betriebssystemverschlüsselung eine Kompatibilität mit zahlreichen unterschiedlichen Kernel-Treibern sowie wertvolle CPU-Zeit erfordert, ist die laufwerksbasierte Verschlüsselung einfach und sicher. In vielerlei Hinsicht glauben wir, dass SEDs die grundlegende Lösung für die Laufwerksverschlüsselung sind. Obwohl sie aufgrund der neuesten Virtualisierungstechnologie und sicheren Workloads in einigen Bereichen weniger geeignet sind, sind wir doch überzeugt, dass SEDs die Grundlage für in IT-Systemen gespeicherte Daten bilden sollten.

Warum ist dies so wichtig?
Unternehmen investieren trotz der Verfügbarkeit der Verschlüsselung auf Betriebssystemebene weiterhin stark in die Laufwerksverschlüsselung. Bei SEDs gibt es noch immer „Kinderkrankheiten" wie Kompatibilitätsprobleme, BIOS u. a. WinMagic zeichnet sich jedoch als echter Pionier auf diesem Gebiet aus. Unser Ruf und unsere starken Beziehungen zu SED- und PC-Herstellern lassen auf eine erfolgreiche Zukunft hoffen.

Sichere virtualisierte Workloads – eine zukunftsweisende Technologie. Unternehmen zögern oft, ihre sensiblen Daten in die Cloud zu übertragen, da sie Bedenken in Bezug auf die Vertraulichkeit, Risiken im Hinblick auf eine mögliche Offenlegung, den Zugang durch Cloud-Serviceanbieter (CSPs), Infrastrukturschwachstellen und das Risiko eines nicht offengelegten Behördenzugangs haben. CSPs wiederum sind besorgt über ihre Haftung im Falle einer Datenschutzverletzung und über einen Vertrauensverlust seitens ihrer Kunden.

Ein Lösungsansatz für dieses Problem sind Speicher-Verschlüsselungstechnologien wie Secure Encrypted Virtualization (SEV) zum Schutz von verwendeten Daten. Im Falle eines SEV-Zugriffs auf unverschlüsselte Klartextdaten steht der Speicher nur der virtuellen Maschine des Kunden (d. h. dem „Gast") zur Verfügung, nicht aber dem CSP-Hypervisor, der Managementsoftware und den Administratoren.

Warum ist dies so wichtig?
Der Schutz der Vertraulichkeit der verwendeten Daten ohne Schutz der gespeicherten Daten stellt keine umfassende Lösung dar. Im Allgemeinen haben Workloads auf einer Festplatte ihren Ursprung, verarbeiten Daten im Speicher (verwendete Daten) und schreiben sie auf die Festplatte (gespeicherte Daten). Die In-Guest-Laufwerksverschlüsselung nutzt die CPU und den Speicher, um gespeicherte Daten zu schützen, und kann vom SEV-Schutz profitieren.

Hier ist der Ansatz von WinMagic entscheidend. Wir ermöglichen es dem Kunden (Gasteigentümer), zu überprüfen, ob seine virtuelle Gast-Workload mittels SEV geschützt ist, BEVOR alle auf der Festplatte gespeicherten vertraulichen Daten freigeschaltet werden und die Workload lädt. Wir glauben, dass die sichere Workload-Technologie, bei der SEV zusammen mit der Laufwerksverschlüsselung und der führenden Schlüsselverwaltung von WinMagic zum Einsatz kommt, die Art und Weise revolutionieren wird, wie Daten in der Cloud und darüber hinaus geschützt werden und so die Datensicherheit für Cloud-Service-Provider und SaaS-Anbieter komplett verändert.

Sichere Datenfreigabe durch Blockchain-basierte DPKI. Der sichere und einfache Austausch von Daten innerhalb des Unternehmens und mit externen Partnern ist schwierig und mit hohen administrativen Kosten verbunden. Bestehende Lösungen verlassen sich auf unsichere Passwörter und erfordern, dass der Benutzer selbst Konten anlegt oder eine bestimmte Methode wie E-Mail oder Dropbox zur Übertragung verwendet.

Warum ist dies so wichtig?
WinMagic kann dieses Problem mit einer Kombination aus Dateiverschlüsselung und symmetrischem Key-Management-Know-how gepaart mit der neuen Blockchain-basierten DPKI-Technologie (Decentralized Public Key Infrastructure) lösen. Unsere Vision ist es, es Benutzern (im Gegensatz zu Administ-

ratoren) zu ermöglichen, Freigabegruppen zu erstellen und zu verwalten. Diese Gruppen kombinieren symmetrische Schlüsselverschlüsselungs-Keys für die unternehmensinterne Freigabe und Public-Key-Kryptografie für die externe Freigabe. Öffentliche Keys werden in der Blockchain-basierten DPKI gespeichert. So werden viele der Mängel herkömmlicher zentralisierter PKI-Systeme behoben. Verschlüsselte Dateien können auf jede beliebige Weise (USB, E-Mail, Box usw.) ausgetauscht werden. Die Empfänger benötigen kein Passwort, um auf die Daten zuzugreifen. Gerät eine Datei in die falschen Hände, kann sie nicht gelesen werden, da der dazu nötige Entschlüsselungs-Key fehlt.

Einheitliche, intelligente Schlüsselverwaltung – die Antwort auf die aktuelle Datensicherheitskrise. Im Vergleich zu herkömmlichen Schlüsselverwaltungssystemen, die als einfacher Key-Speicher fungieren, ist unsere Schlüsselverwaltungslösung intelligent und kontextabhängig. Unter Berücksichtigung von Benutzern, Geräten und Authentifizierungsverfahren kann sie auf intelligente Weise bestimmen, ob der Zugriff gewährt werden soll, wenn ein Key angefordert wird. Die Lösung übernimmt zudem die sichere Schlüsselspeicherung am Endpunkt, stellt die Datensicherheit auch bei Diebstahl oder im Missbrauchsfall sicher und schützt die Schlüsselbereitstellung – und das alles vor dem Betriebssystemstart. Die Vorteile für Anwendungsanbieter sind enorm, was zu besseren, sichereren Produkten für die Kunden führt.

Warum ist dies so wichtig?
SecureDoc von WinMagic ist die einzige Lösung am Markt, die Verschlüsselung und Schlüsselverwaltung für Laufwerke, Dateien und Container für Windows, Linux und Mac für Endpunkte, das IoT, Server, Rechenzentren und die Cloud bietet – mit einer zentralen Übersicht. Da die Schlüsselverwaltung komplex ist, könnten andere Anbieter von unserer Schlüsselverwaltung profitieren, wenn es ein Toolkit gäbe, das sie nutzen könnten. Die Verschlüsselung ist von Natur aus schwierig, wurde aber „einfach“, als es ein entsprechendes Toolkit gab. Das gleiche würde auch für die Schlüsselverwaltung gelten.

Ein Blick in die Zukunft

Wir entwickeln seit 21 Jahren überlegene und benutzerfreundliche Verschlüsselungslösungen und sind stolz auf unsere Leistung. Unsere Philosophie vereint die Informatik mit einer benutzerfreundlichen Denkweise und hat dem Markt gut gedient. Darüber hinaus hat sie es uns ermöglicht, die Datensicherheit für Unternehmen in aller Welt zu verbessern und zu vereinfachen. Das Produktportfolio von WinMagic bietet nach wie vor eine umfassende Datensicherheitslösung, die ihresgleichen sucht. Durch Engagement, unseren Fokus und harte Arbeit werden wir unserem Leitbild treu bleiben: Daten weltweit mit hohen Standards und einer ausgeprägten Ethik zu schützen.

Wir hoffen, dass dieses Vision Statement deutlich gemacht hat, warum wir der Meinung sind, dass WinMagic in der Lage ist, der weltweit führende Anbieter von einheitlichen, intelligenten Verschlüsselungslösungen zu werden. Wir blicken optimistisch in die Zukunft.

Thi Nguyen-Huu
Gründer und CEO, WinMagic