STORMSHIELD



Datenschutzlösungen

Auf dem Weg zu einem Einsatz ohne Einschränkungen?

Juli 2022

DATENSCHUTZ

Jeden Tag müssen die IT-Abteilungen und ihre Teams Updates, Sicherheitspatches und neue Anwendungen einspielen oder einen Computer beim Eintritt eines neuen Mitarbeiters konfigurieren. Diese Vorgänge sind nicht ohne Risiko.

Alle diese Vorgänge sind zeitaufwendig und können zu Fehlern oder Blockaden führen, die sich auf die Geschäftstätigkeit des Unternehmens auswirken. Um agiler zu sein, haben immer mehr Organisationen beschlossen, von „klassischen" Desktops - mit ihren vielen Fat Clients - auf Thin Clients oder virtuelle Desktop-Computer umzusteigen.

Diese Entwicklung darf jedoch nicht auf Kosten des Datenschutzes gehen, der durchgehend verschlüsselt sein muss, um die Vertraulichkeit der Daten zu gewährleisten. Die Nutzererfahrung, oder besser gesagt die Mitarbeitererfahrung, darf ebenfalls nicht vergessen werden, da diese Verschlüsselung auf eine für die Unternehmen möglichst transparente Weise erfolgen muss. Die zunehmende Nutzung von SaaS-Anwendungen zwingt die Hersteller von Sicherheitslösungen, innovativ zu sein und insbesondere eine Lösung für die Datenverschlüsselung als Dienstleistung anzubieten.

Dies ist eines der Versprechen der Stormshield Data Security-Lösung.

Stormshield
Stormshield, der europäische Marktführer für Cybersicherheit und eine 100%ige Tochtergesellschaft von Airbus Defense & Space Cyber Programmes bietet **vertrauenswürdige Lösungen**, die auf höchstem europäischen Niveau zertifiziert und qualifiziert sind. Er ist derjenige Anbieter, der den größten Schutzbereich unter den Inhabern der Sicherheitsvisa der französischen Behörde für Informationssicherheit ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) abdeckt.

Inhalt

04 **Die Verwaltung von Arbeitsplätzen und Software: immer wieder eine Herausforderung**

05 **Kosten der Softwarebereitstellung**

06 **Ist das goldene Zeitalter der schwerfälligen Anwendungen vorbei?**

07 **Rückmeldungen aus der Praxis**

08 **Eine höhere Datensicherheit mit weniger Einschränkungen**

09 **Stormshield Data Security: der agentenlose Verschlüsselungsservice**

10 **Die wichtigsten Punkte**

Die Verwaltung der Desktop-PCs und der Computerprogramme: **Immer wieder eine Herausforderung**

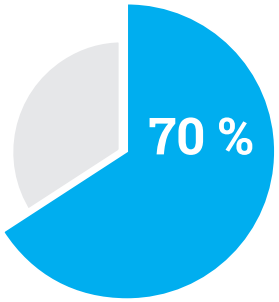
Der Tod des Desktop-PCs wird seit Jahren vorhergesagt. Aber man kommt nicht umhin festzustellen, dass diese historischen Computerarbeitsplätze – PCs und Macs – in den Organisationen immer noch unverzichtbar sind, obwohl sie die Schwerfälligkeit des IT-Managements symbolisieren. Dies ist darauf zurückzuführen, dass die Bereitstellung und Aktualisierung verschiedener Betriebssysteme und Computerprogramme zu oft umständlich, riskant, zeitaufwendig und teuer ist.

Nicht mehr unterstütztes Betriebssystem, neue Anforderungen, Inkompatibilität mit einer Version einer anderen Software, Konflikte mit einer von einem Mitarbeiter installierten Anwendung... Die Verwaltung von Desktop-PCs ist ein Hindernisparcours, wobei die Hindernisse alle Betriebssysteme von Windows über Linux bis hin zu MacOS betreffen. In der Tat können sich viele Faktoren negativ auf die Zeitspanne auswirken, die für die Bereitstellung von Anwendungen und Patches benötigt wird. In der Praxis kann es mehrere Monate dauern, bis ein Computerpark vollständig aktualisiert ist.

Aber das Betriebssystem ist nicht der einzige Faktor, der die Aufgabe der IT-Abteilungen erschwert. Eine einfache Überprüfung des Fat Client-Parks kann ergeben, dass Dutzende, oft sogar Hunderte von Arbeitsplätzen nicht mit den verfügbaren Updates und Patches für gängige Software (wie Java, Adobe Reader und andere) ausgestattet sind. Die Bereitstellung von Updates und die Installation neuer Anwendungen sind jedoch wichtige Schritte, um die Sicherheit des Informationssystems (IS) zu erhöhen und die Anforderungen der Geschäftsbereiche zu erfüllen.

Softwarebereitstellung und **digitale Transformation**

Um die Komplexität der Verwaltung der Desktop-PCs und der Computerprogramme zu bewältigen, verlagern sich die Projekte zur digitalen Beschleunigung zunehmend auf Cloud-Plattformen. Laut einer Studie von IDC im Jahr 2021 wird diese Art von Lösung als strategische Investition in Modernisierungsprojekte gesehen, mit einem Wachstum von 22 % gegenüber 5 % bei den IT-Investitionen insgesamt.



70 % der Anwendungen werden bis 2024 Cloud-nativ sein[1].

In Bezug auf die IT definiert sich der TCO (*Total Cost of Ownership*) als die Summe der Kosten für den Erwerb, die Implementierung, die Verwaltung, den Support und die Nutzung der Technologie. Der Kaufpreis eines Computers ist nur eine Komponente der Kosten eines Geräts während seines gesamten Lebenszyklus.

Für die IT-Abteilung, die häufig noch als reine Kostenstelle betrachtet wird, stellen diese TCO für Kauf und Betreuung eine sehr wichtige finanzielle Position dar. Die Optimierung dieser Kosten führt dazu, dass Unternehmen schnell in die Cloud migrieren. Laut derselben IDC-Studie wird der Anteil der Cloud-nativen Anwendungen dank der Einführung von Technologien wie Microservices, Containern, Orchestrierung und DevOps bis 2024 von 10 % auf 70 % steigen.

[1] Quelle: Artikel von IDC für EasyVista - Mai 2021: https://www.easyvista.com/fr/rapport-idc-service-client-et-support-it

Ist das goldene Zeitalter der **großen Anwendungen** vorbei?

Die „klassischen“ Desktop-PCs bieten eine Vielzahl von Optionen. Aber ihre Verwaltung bleibt schwerfällig und kompliziert. Was wäre, wenn die Lösung in Thin Clients läge, die einfacher zu bedienen, billiger in der Anschaffung und aus der Ferne verwaltbar



Unternehmen setzen für ihre Computeranlagen nicht mehr nur auf die Betriebssysteme von Microsoft. Professionelle Anwender verbinden sich auch mit Unternehmensnetzwerken und Datenquellen über Geräte, die unter iOS und Android laufen, in manchen Bereichen sogar unter MacOS oder Linux, oftmals weil sie sich mehr Geschwindigkeit und Agilität versprechen. Dieser Wunsch nach mehr Agilität zeigt sich auch in der Verwendung von Thin Clients anstelle von Fat Clients.

Das Herunterladen und Installieren von Software von der Website eines Herausgebers oder eines Masters ist eine in den Anfängen entstandene und mittlerweile überholte Praxis, die mit dem Aufkommen von App-Stores wie Google, Apple oder Microsoft einen ersten schweren Schlag erlitten hat. Kurz darauf haben die ersten Generationen von Thin Clients diesen Trend noch verstärkt – als Webanwendung ermöglichen diese Thin Clients den Nutzern den Zugriff auf die meisten ihrer Tools über einen einfachen Browser, auch von anderen Plattformen als Windows, wo Thin Clients oft nicht unterstützt werden.

Die Situation hat sich also verändert, da die neuen Generationen von Thin Clients und ihre Cloud-Anwendungen wie Salesforce, Microsoft Office 365 oder Google Workspace an Bedeutung gewinnen. All diese Anwendungen werden zunehmend in Unternehmen im SaaS-Modus (*Software-as-a-Service*) integriert. Laut einer Studie von Syntec Numérique/IDC[1] boten Ende 2018 78 % der Anbieter dieses Modell an. Für die IT-Abteilung besteht somit das Versprechen aus einer vereinfachten und zentralen Verwaltung von Endgeräten und Software . Eine Realität, in der es möglich ist, automatisch Profilstrategien auf Gruppen von Thin Clients anzuwenden, die auf die gleiche Weise konfiguriert sind. Die Idee ist es, einen „Standard“-Arbeitsplatz zu haben.

Diese Idee weiterführend, entstand das Konzept des *Desktop-as-a-Service* (DaaS). Hier ist es der Anbieter des Dienstes, der direkt die Verwaltung der technologischen Infrastruktur übernimmt: Ressourcenbereitstellung, Lastausgleich, Verwaltung von Netzwerkproblemen usw. Diese Vorteile entbinden die IT-Abteilung jedoch nicht davon, weiterhin die virtuellen Desktops zu verwalten, auf das Desktop-Offset-Protokoll zu achten und die Lizenzen zu kontrollieren.

[1] Quelle: Pressemitteilung von Syntec Numérique - 6. Dezember 2018: https://syntec-numerique.fr/sites/default/files/Documents/2018_12_06_Communique_de_presse.pdf

Rückmeldungen aus der Praxis

Der Arbeitsplatz ist immer noch das Herzstück des Informationssystems aller Organisationen. Aber jede Organisation hat ihre eigenen Ziele und Herausforderungen, die sich um die Benutzererfahrung drehen.

Standardisierung des Arbeitsplatzes in der Welt der Luftfahrt.

Das Ziel dieser ersten Maßnahme ist einfach: Die Auswirkungen des Softwaremanagements (Bereitstellung von Sicherheitspatches, Migration zu einer neuen Version...) auf die Aktivitäten der Mitarbeiter abzuschwächen. Auf lange Sicht sollen damit alle Vorgänge auf den Desktops bequem, schnell und transparent gemacht werden.

Um diese doppelte Herausforderung zu meistern (Senkung der Wartungskosten und der Implementierungen), zielt diese Organisation auf eine „Standardisierung" des Desktops ab, so dass keine On-Demand-Anwendungen oder zusätzliche Schichten mehr verwaltet werden müssen. Unabhängig vom Geschäftsprofil würde jeder Nutzer über einen eigenen Rechner verfügen, dessen Konfiguration aber eine gemeinsame ist.

Vereinfachung des Einsatzes in der Welt der Beratung und Dienstleistungen

Bei einer solchen weltweiten Organisation gibt es eine sehr hohe Fluktuation und sie muss daher fast täglich Abgänge verkraften. Um eine minimale Ausfallzeit der Arbeitsplätze zu gewährleisten, muss das IT-Team einen Desktop somit sehr schnell neu installieren. Dies setzt voraus, dass die Verwaltung möglichst wenig komplex und anpassbar sein muss.

Um Neueinsteiger nicht zu benachteiligen, sollten Anwendungen und Daten über einen Browser und bei Bedarf zugänglich sein, wie es die Google Workspace-Umgebung bietet.

Die Nutzung von App-Stores in der industriellen Welt.

Bei diesem internationalen Konzern sind Anwendungen wie Outlook nicht mehr für seine Organisationsform geeignet. Er bevorzugt nun Outlook Web Access, um von weniger schwerfälligen Desktops zu profitieren und die Interaktion mit anderen Anwendungen auf dem Arbeitsplatz zu reduzieren. Ziel ist es, den Mitarbeitern den Zugriff auf ihre Daten von überall und von jedem Endgerät aus zu ermöglichen.

Allgemein soll somit der Einsatz von Fat Clients auf jedem Terminal zugunsten von Lösungen, die über einen Browser zugänglich sind, eingeschränkt werden. Um die Auswirkungen der Einführung „klassischer" Lösungen zu mildern, hat das Unternehmen beschlossen, sich auf Standardtools zu stützen. Die Teams können auf den SharePoint Store zugreifen, um Anwendungen zu abonnieren.

Höhere Datensicherheit **mit weniger Einschränkungen**

Der Trend zur Nutzung von SaaS-Anwendungen am Arbeitsplatz hat daher zumindest in einem ersten Schritt – die Erwartungen der Nutzer und der IT-Teams erfüllt. Für den Datenschutz und die Hersteller von Sicherheitslösungen besteht die Herausforderung darin, weniger intrusive, aber ebenso wirksame Lösungen anzubieten.



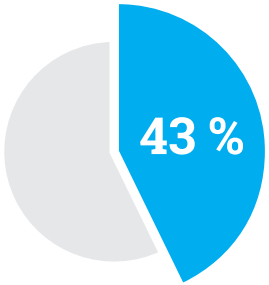
Unabhängig von der Abteilung haben die Mitarbeiter heute einen datenzentrierten Ansatz, der die Daten in den Mittelpunkt ihres Geschäfts stellt. Mit der Hyperverbindung hat sich der Arbeitsbereich des Unternehmens grundlegend verändert: Daten werden ständig zwischen internen Abteilungen und externen Partnern ausgetauscht. Gleichzeitig setzt die Mobilität der Teams voraus, dass der Zugriff auf Daten von jedem Ort und von verschiedenen festen und mobilen Endgeräten aus möglich sein muss. Deshalb wird es umso unabdingbarer, die Sicherheit in die Tools zu verlagern, die diesen Zugriff ermöglichen, in diesem Fall die Browser, und die Verschlüsselung zu verallgemeinern.

Diese Mitarbeiter akzeptieren jedoch immer weniger Einschränkungen, die sie als unnötig oder unverhältnismäßig empfinden. Zu diesen Einschränkungen gehören aber auch solche, die in der Cybersicherheit begründet sind. Außerdem wird die notwendige allgemeine Verschlüsselung von Daten immer noch durch das Vorurteil behindert, dass Verschlüsselung kompliziert sei. Da jede neue Lösung oder jedes neue Verfahren nur dann gut ist, wenn sie/es verstanden, angenommen und beherrscht wird, ist es unerlässlich, die Nutzer über den besonderen Charakter von Daten und die Einfachheit der Verschlüsselung aufzuklären. Der CIO muss hier eine wichtige Rolle spielen, da er ein wichtiges Element der Datenschutzstrategie darstellt.

Und diese (R)Evolution betrifft auch die Sicherheitsanbieter in diesem Bereich. Nach den Fat Clients aus den Anfängen der Cybersicherheit muss man heute intuitive und einfach zu bedienende Lösungen anbieten. Das Ziel ist es, diejenigen Endnutzer zufrieden zu stellen, die Verschlüsselung immer noch als Einschränkung empfinden. **Und wenn der Schlüssel zur digitalen Transformation im Vertrauen der Mitarbeiter auf interner Ebene – und der Kunden auf externer Ebene – in der Fähigkeit der Organisation läge, die ihnen anvertrauten Daten zu schützen?**

Stormshield Data Security: **die SaaS-Verschlüsselungslösung.**

Der Datenschutz muss weiterhin Priorität haben. Um die Erwartungen der IT-Teams zu erfüllen, ist es jedoch wichtig, sich auf Lösungen zu verlassen, die dem Trend zu Thin Clients folgen. Und für die Mitarbeiter müssen die Erwartungen an die Ergonomie und die Benutzerfreundlichkeit erfüllt werden. All diese Versprechungen und Funktionen sind in der neuen Lösung von Stormshield Data Security, Ihrem SaaS-Datenverschlüsselungsprodukt, enthalten.



43 % der Organisationen erkennen die Bedeutung einer umfassenden Verschlüsselungsstrategie an.

Die Datensicherheit ist in einem Umfeld, das von starkem Wettbewerb und zunehmenden Datenlecks geprägt ist, mehr denn je von entscheidender Bedeutung. Dieses Ziel erfordert eine allgemeine Verschlüsselung, um die Vertraulichkeit bestimmter kritischer Dokumente und Ordner, die online geteilt oder über E-Mail ausgetauscht werden, stärker zu schützen.

Die allgemeine Verschlüsselung von Dokumenten und E-Mails ist umso wichtiger, je mehr Unternehmen einen Teil ihres Informationssystems oder ihrer Anwendungen in die Cloud verlagern. Der neue Service vonStormshield Data Security reagiert auf diese Entwicklung, indem er sich vollständig in die Arbeitsumgebung von Google Workspace integriert, um die Vertraulichkeit der ausgetauschten Daten zu gewährleisten. Dabei ist es nicht notwendig, eine aktualisierte Version auf den Computern Ihrer Mitarbeiter zu installieren und zu pflegen. Die vertrauenswürdige End-to-End-Verschlüsselung wird unter der alleinigen Kontrolle des Unternehmens durchgeführt, bevor die Daten auf den Servern der Cloud-Plattform gespeichert werden. Der Administrator hat keinen Zugriff auf diese Daten.

Das SaaS-Angebot von Stormshield Data Security für Google Workspace ist ein schlüsselfertiger und eigenständiger Datenschutzservice. Die Ver- und Entschlüsselungsprozesse sowie die Verwaltung der Benutzerschlüssel werden vollständig von Stormshield übernommen.

[1] Quelle: Studie „Global Encryption Trends", Ponemon - April 2018.

Was Sie sich merken sollten

Mit der zunehmenden Verbreitung von mobilen Geräten und neuen Webanwendungen haben die IT-Abteilungen den Wert **einfacher und intuitiver Benutzeroberflächen erkannt**.

Die Mitarbeiter interessieren sich nämlich nicht so sehr für die Technologie, sondern für die Agilität, die sie bietet. Um dies zu erreichen, werden sich immer mehr Unternehmen auf intuitive Webanwendungen und kollaborative Tools verlassen. **Dies verspricht einen schnelleren Datenaustausch und Zugriff auf Daten**.

Die Frage des Datenschutzes wird oft als lästige Pflicht angesehen, sollte aber nicht unterschätzt werden – weder für die Nutzer noch für ihre IT-Teams. Dieses Thema der Cybersicherheit muss eine der Prioritäten der IT-Abteilungen bleiben, um **die Daten zu schützen, ohne ihre Zugänglichkeit zu beeinträchtigen**. Die Integration der End-to-End-Verschlüsselung in den Browser und die intuitive Bedienung der Anwendung werden die ersten Antworten bei dieser Zielsetzung sein.

Der Erfolg dieser wichtigen Entwicklung in der Herangehensweise an die Cybersicherheit wird von der Akzeptanz der Mitarbeiter abhängen. Daher **wird die Änderung der Mentalität gegenüber der Verschlüsselung** in den kommenden Jahren eine große Herausforderung für die IT-Abteilungen darstellen.

Cloud-Computing ist bereits die neue Norm. Und es ist die Unternehmenskultur, die den Übergang blockiert, nicht die Technologie...



STORMSHIELD

Überall auf der Welt müssen Unternehmen, Regierungsbehörden und Verteidigungsorganisationen die Cybersicherheit ihrer kritischen Infrastrukturen, sensiblen Daten und Betriebsumgebungen gewährleisten. Die Technologien von Stormshield sind auf höchster europäischer Ebene zertifiziert und erfüllen die IT- und OT-Anforderungen, um ihre Aktivitäten zu schützen. Unsere Mission: **Die Cyber-Sicherheit unserer Kunden** gewährleisten, damit sie sich auf ihr Kerngeschäft konzentrieren können, das so entscheidend für das reibungslose Funktionieren unserer Institutionen, unserer Wirtschaft und der Dienstleistungen für die Bevölkerung ist. **Mit der Wahl von Stormshield setzen Sie auf einen vertrauenswürdigen Anbieter für Cybersicherheit in Europa.**

Weitere Informationen finden Sie unter:
www.stormshield.com

www.stormshield.com



Copyright Stormshield - 2018-2022