SHARP

Zoellner

Richtlinien sind beim Thema Datensicherheit nicht genug. Unlock: Erschließen Sie daher eine Kultur der Sicherheit in Ihrem Unternehmen.

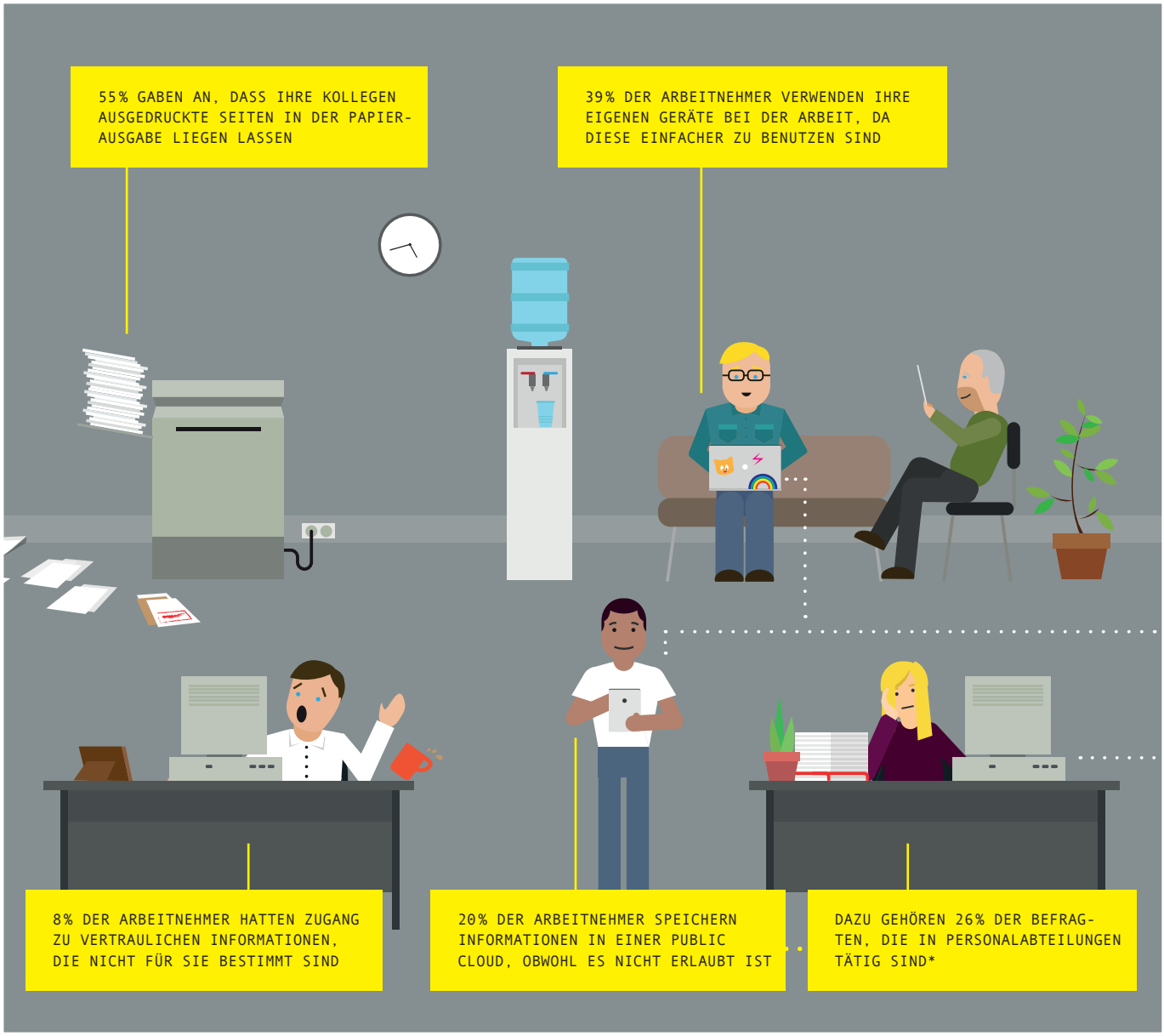
MEHR ALS 21 % DER BÜROANGESTELLTEN IN EUROPA NUTZEN UNAUTORISIERTE FILE-SHARING-DIENSTE FÜR SENSIBLE DOKUMENTE*

Laut unserer Umfrage unter Büroangestellten, achten viele Mitarbeiter nicht auf Datensicherheitsrichtlinien. Bis Unternehmen dieses Problem nicht beheben, besteht die Gefahr von vermeidbaren Sicherheitsverletzungen. Prüfen Sie im Folgenden, wie Sie im Vergleich mit anderen Firmen abschneiden.

*Studie vom April 2016, durchgeführt durch Censuswide im Auftrag von Sharp Europe

Nimmt Ihr Büro das Thema Datensicherheit ernst?

Die Umfrage unter 6.000 Büroangestellten in ganz Europa hat ergeben, dass viele Menschen die Sicherheitsrichtlinien nicht beachten. Wenn Unternehmen dieses Problem nicht beheben, besteht die Gefahr von vermeidbaren Sicherheitsverletzungen, die zu Sanktionen, Verlust von geistigem Eigentum und Unannehmlichkeiten für die Mitarbeiter führen können.



* 457 Befragte gaben an, dass sie in einer Personalabteilung arbeiten.

Nimmt Ihr Büro das Thema Datensicherheit ernst?

Unsere Umfrage wurde unter 6.045 Büroangestellten in neun EU-Ländern durchgeführt (Frankreich, Deutschland, Vereinigtes Königreich, Italien, Schweden, Polen, Niederlande, Tschechien und Ungarn). Darunter 1.015 in Deutschland. Ein paar Fakten aus der Studie zum Thema „Datensicherheit“ finden Sie nachstehend:

- Fast jeder zehnte Arbeitnehmer **(8 %)** gab an, Zugang zu vertraulichen Informationen zu haben, die nicht für ihn bestimmt sind.
- **21 %** sagten, dass sie ohne die Genehmigung des Unternehmens öffentliche File-Sharing-Dienste verwenden.
- Fast ein Drittel der Befragten **(29 %)** gab zu, die Bürorichtlinien zu ignorieren und Arbeit mit nach Hause zu nehmen, um sie dort zu beenden.
- Die Nichtbeachtung der Firmenrichtlinien ist ein verbreitetes Problem: Ein Fünftel der befragten Arbeitnehmer **(20 %)** gab zu, arbeitsbezogene Informationen in einer Public Cloud zu speichern, obwohl es nicht erlaubt ist.
- Darunter befanden sich **26 %** der Befragten, die in Personalabteilungen arbeiten und dadurch potenziell persönliche Daten gefährden*.

Sicherheitsrichtlinien sind nicht genug. /This is Why: Darum sollten Sie einen persönlichen Ansatz verfolgen.

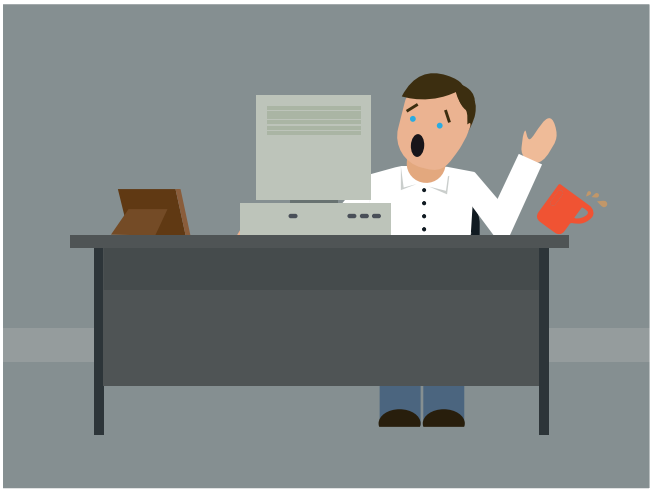
Wir haben **Dr. Karen Renaud, Expertin für Sicherheit und Datenschutz,** darum gebeten zu erklären, warum der Datensicherheit seitens der Arbeitnehmer augenscheinlich keine hohe Priorität eingeräumt wird. Im Folgenden erklärt Dr. Renaud, wie Unternehmen diesen Umstand ändern können, um sicherzustellen, dass sie vor externen und internen „Zugriffen" geschützt sind.

„Ich war von den Ergebnissen der Sharp-Umfrage nicht überrascht. Tatsächlich stützt sie andere Untersuchungen des Pew Research Centre in den USA zur Einstellung in Bezug auf Sicherheit und persönliche Daten.

Mitarbeiter haben die Verantwortung, auf Sicherheit zu achten. Allerdings glaube ich nicht, dass Arbeitgeber ihren Pflichten dabei auch wirklich nachkommen. Viele kleine Unternehmen schließen das Thema Sicherheit einfach dadurch ab, dass sie ihre Mitarbeiter auffordern, eine Sicherheitsrichtlinie zu unterzeichnen. Dabei ist es unrealistisch zu denken, dass es ausreicht, den Mitarbeitern einfach eine Liste mit Anweisungen zu geben.

Stattdessen muss ein persönlicher Ansatz verfolgt werden. Dazu gehört auch, die Tatsache zu akzeptieren, dass es menschlich ist, fehlbar zu sein – und alle Anweisungen der Welt werden nicht dazu beitragen, sichere Verhaltensweisen zu gewährleisten.

Was fehlt, ist eine Lösung, die auf Technologie und Schulungen gleichermaßen setzt.



8% DER ARBEITNEHMER HATTEN ZUGANG ZU VERTRAULICHEN INFORMATIONEN, DIE NICHT FÜR SIE BESTIMMT SIND

Warum wir Sicherheit nicht ernst nehmen

Viele Unternehmen denken, dass sie das Problem der Sicherheit mit schriftlichen Richtlinien lösen können. Ich bin jedoch davon überzeugt, dass wir dabei etwas realistischer sein sollten: Menschen zu kontrollieren und sie dazu zu bringen, etwas auf eine bestimmte Weise zu tun, ist eine sehr komplexe Herausforderung. Vor allem dann, wenn es dabei um gewohnheitsmäßige Tätigkeiten geht.

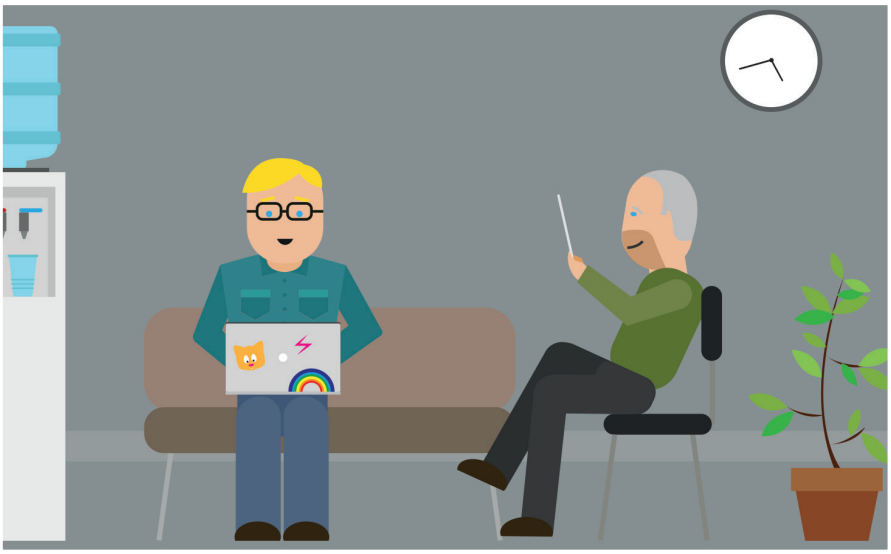
Als Menschen erlernen wir neue Fähigkeiten und jedes Mal, wenn wir das gelernte Verhalten wiederholen, wird es mehr und mehr verinnerlicht. Alles, was wir regelmäßig tun, übernimmt der für Automatismen zuständige Teil des Gehirns.

Aus diesem Grund ist es z. B. auch unrealistisch, seine Mitarbeiter zu bitten, jede E-Mail sorgfältig dahingehend zu überprüfen, ob es sich um eine Phishing-E-Mail handelt. Denn: Wir gehen davon aus, dass etwas in Ordnung ist, wenn es normalerweise in Ordnung ist.

Ein weiteres Problem ist, dass Mitarbeiter angewiesen werden, auf bestimmte Weise zu agieren und zu reagieren, gleichzeitig aber im Unternehmen mit widersprüchlichen Informationen konfrontiert werden, beispielsweise bei E-Mails: Unternehmen bitten ihre Mitarbeiter, mit Links vorsichtig umzugehen. Dennoch senden sie häufig interne E-Mails mit Links, auf die die Mitarbeiter klicken und die sie beachten sollen.

Menschen denken oft, dass ihnen keine Sicherheitsverletzung unterläuft, weil sich das menschliche Gehirn nicht so schnell entwickelt hat wie die Technologie. Wir haben gelernt, auf Dinge zu reagieren, die uns sofort schaden. Deshalb ist es für den Einzelnen schwer, die Folgen unzureichender Sicherheit vorherzusehen, wenn es keine unmittelbaren Konsequenzen gibt. Wählt jemand zum Beispiel ein schwaches Passwort und nichts passiert, wird diese Person weiterhin schwache Passwörter verwenden und diese Art des Denkens prägt sich ein. Wir glauben nicht, dass als Konsequenz aus unseren Tätigkeiten eine Sicherheitslücke entstehen wird.

39% DER ARBEITNEHMER VERWENDEN IHRE EIGENEN GERÄTE BEI DER ARBEIT, DA SIE EINFACHER ZU BENUTZEN SIND



Aufbau einer Sicherheitskultur

Menschen lernen, indem sie sehen, wie sich andere Personen in einer Organisation verhalten. Genau darauf sollten sich Unternehmen konzentrieren: den Aufbau einer Kultur der Sicherheit.

Das kann sehr einfach mit den richtigen Schulungen beginnen. Allerdings müssen Sie hierbei sicherstellen, dass diese nicht nur relevant, sondern auch interessant und abwechslungsreich sind. Man kann nicht einfach Leute bitten, einem Webinar zu folgen und dann erwarten, dass allein hierdurch eine Veränderung eintritt.

Unternehmen sehen Schulungen leicht als „Impfstoff" und glauben: „Wir haben alle geimpft, daher sind wir jetzt immun". Allerdings wissen wir aus Erfahrung, dass der Schulungseffekt und das sicherheitsbewusste Verhalten mit der Zeit nachlassen, die Auflagen lästig und die Mitarbeiter wieder nachlässiger werden. Man kann also das Bewusstsein nicht nur einmal schaffen, man muss die entsprechenden Schulungen kontinuierlich durchführen und darauf achten, das geschaffene Bewusstsein zu fördern. Mitarbeiter müssen die sicherheitsrelevanten Themen verstehen und wissen, warum sie wichtig sind, da sie ein Gleichgewicht zwischen Sicherheit und der Erfüllung ihrer Aufgaben schaffen müssen. Für Unternehmen ist dies eine Gratwanderung zwischen übertriebener Sicherheit und unsicherem Verhalten. Sie müssen die Sicherheitslücken ausgleichen, ohne ihre Mitarbeiter davon abzuhalten, ihre Arbeit effektiv zu erledigen. In dem Moment, in dem Sicherheit zu einem Hindernis wird, werden Mitarbeiter versuchen, die Sicherheitsauflagen zu umgehen.

In Unternehmen muss ein Bewusstsein dafür geschaffen werden, dass diese Zustände existieren. In diesem Fall können die Grenzen neu gesteckt und bessere Möglichkeiten gefunden werden, um Sicherheit zu gewährleisten.

21% DER ARBEITER GABEN AN, DASS SIE OHNE DIE GENEHMIGUNG DES UNTERNEHMENS ÖFFENTLICHE FILE SHARING-DIENSTE NUTZEN

Integration von Sicherheit in die Systeme

Beim Erstellen einer Sicherheitsrichtlinie müssen Unternehmen darüber nachdenken, wie sie in ihr System etwas einflechten können, das Unsicherheit verhindert. Auf diese Weise setzt das Unternehmen den Benutzer nur dann dieser Belastung aus, wenn es nicht anders möglich ist.

Drucker sind dafür ein gutes Beispiel, da sie leicht so eingerichtet werden können, dass sie private Daten schützen. In kleinen Büros drucken die Mitarbeiter ihre Dokumente einfach aus und holen die Ausdrucke zu einem späteren Zeitpunkt ab, außer die Arbeit ist sehr dringend. Während dieser Zeit liegen die gedruckten Informationen – ob vertraulich oder nicht – im Ausgabefach und könnten von jedermann eingesehen werden.

Bei vielen Druckern können Sie jedoch eine Sicherheitsebene hinzufügen, z. B. einen Code oder einen ID-Kartenleser am Drucker, der verwendet werden muss, bevor der Druckauftrag bearbeitet wird. Auf diese Weise kann der Benutzer seine Arbeit erst dann drucken, wenn er vor dem Drucker steht. Es macht unsicheres Verhalten unmöglich, ohne dass der Benutzer zusätzliche Anstrengungen unternehmen muss, denn die Ausdrucke muss er ohnehin abholen.

Es gibt viele Sicherheitslösungen wie diese, die in Ihre Büroumgebung integriert werden können. Allerdings müssen Sie dafür über Erfahrung in vielen Bereichen verfügen. Ein Outsourcing an den richtigen Anbieter ist daher für kleine Unternehmen oft ratsam. Von Mitarbeitern mit Spezialisierungen in anderen Bereichen kann nicht erwartet werden, dass sie alles über Cybersicherheit wissen.

55% DER ARBEITNEHMER GABEN AN, DASS IHRE KOLLEGEN AUSGEDRUCKTE SEITEN IN DER PAPIERAUSGABE LIEGEN LASSEN

File Sharing-Dienste

File Sharing-Tools gehören in Unternehmen immer mehr zum Alltag und können für Ihre Informationen ein Risiko darstellen. Anstatt zu versuchen, ihre Verwendung zu verbieten, müssen Sie als Unternehmen herausfinden, warum Ihre Mitarbeiter diese Dienste nutzen und welche Informationen sie dort speichern.

Die meisten Personen benutzen File Sharing-Tools, da es der einfachste Weg ist, um Daten mit Kollegen an einem anderen Standort oder in einer anderen Einrichtung zu teilen. Wenn Sie diese Gründe als berechtigt erachten, müssen Sie Ihren Mitarbeitern eine sicherere Alternative bereitstellen. Tun Sie es nicht, werden ihre Mitarbeiter weiterhin öffentliche Sharing-Websites verwenden. Darüber hinaus werden sie dies heimlich tun, weil sie wissen, dass Sie damit nicht einverstanden sind.

Sharp fand heraus, dass 20 % der Angestellten arbeitsbezogene Informationen in einer Public Cloud speichern, obwohl sie wissen, dass es nicht erlaubt ist. Ich wäre nicht überrascht, wenn diese Zahl in Wirklichkeit noch höher liegt.

Es können jedoch Regeln aufgestellt werden, um diesen Sachverhalt einfacher und klarer darzustellen. Zum Beispiel können die entsprechenden Parameter so eingestellt werden, dass sensible Daten nicht verschoben oder übertragen werden können und an einem speziellen Ort gespeichert sind, während nicht sensible Daten an anderen Orten gespeichert und frei genutzt werden können.

Fazit von Dr. Renaud

Menschen sind keine Computer und können nicht programmiert werden. Ein persönlicher Ansatz ist entscheidend für Ihre Datensicherheit.

Unternehmen sollten Technologie überall dort einsetzen, wo es unerlässlich ist, dass die sicherste Option zur automatischen Option wird. Unternehmen müssen jedoch auch auf das richtige Maß an Kontrolle achten, um ihre Mitarbeiter nicht daran zu hindern, ihre Arbeit effizient zu erledigen. Wenn die Sicherheitsrichtlinien verhindern, dass Mitarbeiter ihre Arbeiten ordnungsgemäß erledigen können, dann ist es Zeit, diese Technologie zu überdenken.

Nur durch die Kombination von Technologie, Schulungen und einem persönlichen Sicherheitsansatz kann ein Unternehmen sicherer werden. Denken Sie jedoch daran, dass es keinen perfekten „Impfstoff" gibt."

20% DER ARBEITNEHMER SPEICHERN INFORMATIONEN IN EINER PUBLIC CLOUD, OBWOHL ES NICHT ERLAUBT IST

Sie kennen jetzt die Expertenmeinung zum Thema Datensicherheit. /This is Why: Darum sollten Sie auf die Empfehlungen von Sharp vertrauen.

Sharp bietet Ihrer Organisation eine breite Palette an Sicherheitslösungen. Sie reichen von Sicherheitsfunktionen, die in der Hardware der Multifunktionsgeräte (MFPs) von Sharp integriert sind, bis hin zu Lösungen für ein sicheres Druck-Management, cloudbasierten Diensten zur Speicherung und gemeinsamen Nutzung von Dateien.

Dokumentenverwaltung und Workflow: Cloud Portal Office

Sharp Cloud Portal Office ist ein preisgekrönter und sicherer Software-Service für Dokumentenmanagement und Kollaboration, damit elektronische Dateien und gescannte Dokumente sicher gespeichert und geteilt werden können. Cloud Portal Office kann sowohl mit den Multifunktionsgeräten als auch mit den interaktiven Display-Systemen BIG PAD von Sharp vollständig integriert werden. Dadurch ermöglicht Cloud Portal Office Ihren Mitarbeitern eine effizientere Arbeitsweise und ist eine sichere Alternative.

Zugriff

Cloud Portal Office bietet Sicherheitsfunktionen, die den Industriestandards für SaaS-Anwendungen (Software as a Service) entsprechen, mit Firewalls, die an den externen und internen Grenzen des Netzwerks installiert sind, um Sie gegen ungesicherte Verbindungen und Traffic zu schützen. Bei der Nutzung von Cloud Portal Office erhalten Firmen eine „Private Instance“ mit Sicherheitsrichtlinien, die vom Unternehmen festgelegt werden können und maximale Sicherheit durch äußere Angriffe und unberechtigten Zugriff bieten.

Sichtbarkeit

Alle Daten auf Cloud Portal Office können von Ihrem IT-Administrator eingesehen werden. Jedes Firmenkonto verfügt über Logins für einen oder mehrere unternehmensweite Administratoren. Diese Admin-Logins werden normalerweise vom IT-Personal verwendet, um Benutzer innerhalb ihrer Unternehmenskonten zu überwachen und zu verwalten.

File-Sharing

Cloud Portal Office ermöglicht Ihnen eine vollständige Kontrolle darüber, wer auf Ihre Dateien zugreifen, sie bearbeiten und freigeben kann. Wenn Sie eine Datei oder einen Ordner mit einem Kollegen teilen, können Sie verschiedene Berechtigungsstufen einstellen, z. B. nur lesen, lesen, schreiben, löschen und teilen. Außerdem können Sie Dateien über eine auslaufende Verbindung auch an Personen senden, die Cloud Portal Office nicht verwenden. Dadurch ermöglichen Sie diesen Personen den Zugang zu Dateien, die sie benötigen, um ihre Arbeit zu erledigen, minimieren jedoch gleichzeitig die Sicherheitsrisiken.

Mobiler Zugriff

Cloud Portal Office bietet Ihnen einen einfachen „On-the-go“-Zugriff auf gespeicherte Inhalte und ein optimales Gleichgewicht zwischen Sicherheit mit Verfügbarkeit. Benutzer von mobilen Geräten mit der Cloud-Portal-Office-App können Dokumente über eine sichere SSL-Verbindung abrufen. Für zusätzliche Sicherheit müssen sich Benutzer authentifizieren, bevor sie auf Daten zugreifen können, ihre Anmeldeinformationen werden auf ihrem Gerät verschlüsselt und auch der gesamte Systemzugriff ist verschlüsselt. Im Falle eines Diebstahls des mobilen Geräts können diese ihr Passwort über den Browser zurücksetzen.

Sicherheit ist in den MFPs von Sharp integriert

Die heutigen intelligenten Multifunktionssysteme und Drucker in Firmennetzwerken verfügen über viele Speicher- und Datenkommunikationsfähigkeiten wie PCs. Daher sollten Sie der Sicherung Ihrer Multifunktionsgeräte genauso viel Aufmerksamkeit widmen wie der Sicherung Ihrer Computer. Multifunktionsgeräte von Sharp verfügen über viele eingebaute Sicherheitsmerkmale, um Sie vor digitalen Bedrohungen zu schützen:

Authentifizierung

Benutzerauthentifizierung und Druckverwaltung bedeuten, dass gedruckte Dokumente nicht in einem Ausgabefach des Multifunktionsgeräts gesammelt und dadurch von jedem Mitarbeiter des Büros abgeholt werden können.

Zugriff

Hacker könnten versuchen, auf sensible Benutzerinformationen und Adressbucheinträge zuzugreifen, die auf einer Festplatte des Multifunktionssystems gespeichert sind. Die Geräte von Sharp bekämpfen diese Bedrohung mit sicheren Administratorpasswörtern, IP- und MAC-Adressenfilterung, Portsteuerung und mehreren Arten der Benutzerauthentifizierung. Das Data Security Kit von Sharp umfasst Datenverschlüsselungstechnologien, die es praktisch unmöglich machen, Restdaten von einem Sharp MFP abzufangen oder wiederherzustellen.

Sicheres Scannen

Ausgewählte Multifunktionsgeräte von Sharp verfügen darüber hinaus über eine Scan-to-Home-Funktion. Diese trägt dazu bei, dass gescannte Bilder ordnungsgemäß gespeichert und sensible Informationen nicht versehentlich gescannt und im falschen Netzwerkordner abgelegt werden.

Der Schutz für sensible Dokumente wird außerdem durch von Sharp verschlüsselte Adobe®-PDF-Dateien zum Scannen und Drucken gewährleistet.

Mobiler Zugriff

Viele Personen nutzen heute mobiles Drucken. Sharp bietet mobilen Benutzern mit der Benutzerauthentifizierung am MFP – einem sicheren, internetbasierten Protokoll – und dem „Halten" des zu druckenden Dokuments, bis sich der Benutzer am Gerät befindet, eine sichere Möglichkeit, sich mit dem Firmennetzwerk zu verbinden.

Prüfprotokoll

Zum Schutz vor Bedrohungen müssen Sie in der Lage sein, jede verdächtige Aktivität zu erkennen. Die detaillierten Prüfpfade und Auftragshistorien von Sharp ermöglichen eine umfassende Auditierung aller Benutzer- und Geräteaktivitäten.

Sichere Entsorgung

Um bei Leasingende sicherzustellen, dass alle Ihre vertraulichen Daten gelöscht und überschrieben werden, bieten die meisten MFPs von Sharp dafür standardmäßige Funktionen.

Optimierte Softwarelösungen: Output-Management

Sharp bietet für alle Arten von Organisationen unabhängig von ihrer Größe Druckmanagementlösungen an, um die Druckkosten zu verwalten und zuzuordnen. Zusätzlich zu den eingebauten Funktionen für Abrechnungscodes und die Druckfreigabe, sind Multifunktionssysteme und Drucker von Sharp kompatibel mit verschiedenen Output-Management-Anwendungen, die Funktionen für eine vereinfachte Zugriffskontrolle und Kostenerstattung bieten. Die Vorteile sind u. a.:

Zugriff

Einfache Authentifizierung über das Netzwerk mit Benutzername und Passwort oder ID-Karte.

Berechtigungen

Verwalten der MFP-Funktionen und des Funktionszugriffs nach Benutzern oder Abteilungen zur Verbesserung der Sicherheit.

Sichtbarkeit

Tracken Sie alle Aktivitäten. Verwalten und überwachen Sie die Druck-, Kopier- und Scan-Aktivitäten, um die Ausgaben zu tracken und Ressourcen zu optimieren.

Kostenerstattung

Durch die Abrechnung an Kunden für die Arbeit, die Sie für sie tun.

Willkommen bei Sharp

Bei Sharp arbeiten wir kontinuierlich an Innovationen, um sicherzustellen, dass wir Unternehmen die umfassendsten Kontrollfunktionen bieten können. Unsere verbundenen Technologien haben die Art und Weise revolutioniert, mit der sich Unternehmen mit Information, Technologie und einander beschäftigen. Diese Möglichkeiten möchten wir auch Ihrem Unternehmen bieten. Finden Sie heraus, wie wir das Potenzial Ihres Unternehmens noch heute steigern können.

SHARP

Inspiring ideas from technology

Zöllner Büro- & IT-Systeme GmbH
Burgstraße 1
D-04910 Elsterwerda
Tel.: +49 3533 4807 0

www.zoellner-office.de

Zoellner