DriveLock idgard® A DRIVELOCK COMPANY

CASE STUDY

Von Schatten-IT zu kontrollierter Sicherheit

Die Transformation von IT und Zusammenarbeit in einer Anwaltskanzlei

Herausforderungen und Ziele

Die israelische Anwaltskanzlei Geller Han Markovitch verarbeitet hochsensible Informationen, darunter Finanzdaten, Rechtsdokumente und personenbezogene Daten (PII). Die Gewährleistung von Datenschutz, Nachvollziehbarkeit, Einhaltung der Datenschutzbestimmungen und sicherer Zusammenarbeit mit externen Parteien ist daher von entscheidender Bedeutung.

Eine zentrale operative Herausforderung betraf den Dokumentenaustausch der Kanzlei mit externen Zustelldiensten („Kuriere"). Rechtsdokumente wurden routinemäßig außerhalb der Organisation übermittelt, physisch zugestellt, von Dritten unterzeichnet und anschließend zusammen mit dem Zustellnachweis zurückgesandt. Dieser Arbeitsablauf stützte sich stark auf manuelle Bearbeitung, E-Mail-Austausch, lokale Dateispeicherung, das Scannen von Dokumenten und administrative Koordination.

Der Prozess war zwar funktionsfähig, beruhte jedoch weitgehend auf vertrauensbasierten Arbeitsabläufen mit begrenzter technischer Durchsetzung, was Risiken in Bezug auf Datenschutz, Rechenschaftspflicht, Nachvollziehbarkeit und Prozesseffizienz mit sich brachte. Das Verwaltungspersonal verbrachte viel Zeit damit, Zustellungen zu koordinieren, den Status von Dokumenten zu verfolgen, zurückgesandte Unterlagen einzuscannen und die damit verbundene Kommunikation zu verwalten.

Gleichzeitig deckte eine von ARMOR360 durchgeführte Endpunktsicherheitsbewertung eine erhebliche Anzahl nicht autorisierter und nicht verwalteter Anwendungen innerhalb der Umgebung auf. Viele dieser Anwendungen waren der Geschäftsleitung völlig unbekannt und stellten ein erhebliches Shadow-IT-Risiko dar, wodurch sowohl das operative Risiko als auch die Angriffsfläche des Unternehmens erhöht wurden.

Auf der Grundlage dieser Erkenntnisse definierte das Unternehmen die folgenden Ziele:

- **Beseitigung des „Shadow-IT"-Risikos**
- **Nur genehmigte Geschäftsanwendungen zulassen**
- **Sicherstellung sensibler externer Kooperationsabläufe**
- **Verbesserung der Nachvollziehbarkeit, Transparenz und Rechenschaftspflicht**
- **Reduzierung des manuellen Verwaltungsaufwands**
- **Wahrung der Benutzerfreundlichkeit und der Betriebskontinuität**
- **Abstimmung von Datenschutz-, Sicherheits-, Compliance- und betrieblichen Anforderungen**

Das übergeordnete Ziel bestand nicht nur darin, die Sicherheitskontrollen zu verstärken, sondern ein durchsetzbares Betriebsmodell zu etablieren, das Sicherheit, Datenschutz, Compliance und Geschäftseffizienz vereint, ohne den täglichen Betrieb zu stören.

DriveLock idgard®

CASE STUDY

Auswahlprozess und Entscheidung für DriveLock und idgard

Das Unternehmen benötigte eine Lösung, die strenge Sicherheitsrichtlinien durchsetzen kann und gleichzeitig die Benutzerfreundlichkeit und die Betriebskontinuität gewährleistet. Eine zentrale Anforderung war die Möglichkeit, präventive Kontrollen zu implementieren, ohne zusätzliche Hürden für Mitarbeiter, Verwaltungsmitarbeiter oder externe Partner zu schaffen.

Nach der von ARMOR360 durchgeführten Bewertung und Workflow-Analyse fiel die Wahl auf die Kombination aus DriveLock und idgard, um sowohl die technischen Sicherheitsherausforderungen als auch die zugrunde liegenden Prozessschwächen zu beheben.

Zu den wichtigsten Entscheidungsfaktoren gehörten:

- **Strenge Kontrolle über die Ausführung von Anwendungen durch Whitelisting**
- **Vollständige Transparenz über die bestehende Anwendungslandschaft**
- **Strenge Durchsetzung bei gleichzeitiger operativer Benutzerfreundlichkeit**
- **Sichere und strukturierte Workflows für die externe Zusammenarbeit**
- **Umfassende Überprüfbarkeit und Rückverfolgbarkeit**
- **Unterstützung von Datenschutz- und Compliance-Anforderungen**

Diese Kombination ermöglichte es dem Unternehmen, Sicherheitslücken zu schließen, operative Risiken zu reduzieren und kritische Geschäftsprozesse durch einen einheitlichen Ansatz zu modernisieren.

ARMOR

DriveLock idgard® A DRIVELOCK COMPANY

Implementierung und Durchführung

ARMOR360, der autorisierte Distributor von DriveLock und idgard in Israel, leitete das Projekt von der Bestandsaufnahme über die Implementierung bis hin zur Einführung und integrierte dabei Sicherheitskontrollen, die Neugestaltung von Arbeitsabläufen und betriebliche Verbesserungen in einer einzigen Transformationsinitiative.

Die Implementierung begann mit der Endpunktsicherheit. Mithilfe von DriveLock wurden strenge Richtlinien für Anwendungs-Whitelists eingeführt, sodass nur ausdrücklich genehmigte Anwendungen ausgeführt werden durften. Dadurch wurde sofort eine große Anzahl nicht autorisierter Tools aufgedeckt, die zuvor ohne Transparenz oder Kontrolle betrieben worden waren.

Alle identifizierten Anwendungen wurden überprüft, kategorisiert, gegebenenfalls genehmigt oder bei Bedarf blockiert. Dies reduzierte das Risiko durch „Shadow IT" erheblich und minimierte die Angriffsfläche des Unternehmens.

Parallel dazu wurde idgard implementiert, um den Prozess des externen Dokumenten-austauschs des Unternehmens zu transformieren. Anstatt sich auf fragmentierte E-Mail-Kommunikation, die lokale Datei -Verarbeitung und manuelle Koordination zu verlassen, konnten sensible Informationen nun über eine strukturierte, sichere und vollständig überprüfbare Kollaborationsumgebung ausgetauscht werden.

Zu den wichtigsten Funktionen gehörten:

- **Identitätsbasierter und zeitlich begrenzter Zugriff**
- **Kontrollierte Zusammenarbeit mit Dritten**
- **Durchgängige Nachvollziehbarkeit und Rückverfolgbarkeit**
- **Automatisierte Löschung und Lebenszyklusmanagement**
- **Verkürzte Zeitfenster für die Offenlegung sensibler Informationen**
- **Sicherer Umgang mit zurückgesandten Dokumenten und Zustellnachweisen**

Das Ergebnis war nicht nur ein sichererer Prozess, sondern ein neu gestalteter Arbeits-ablauf, der die Transparenz, Verantwortlichkeit und betriebliche Effizienz verbesserte und gleichzeitig die Abhängigkeit von manuellen Verwaltungsaufgaben verringerte.

Ergebnisse und geschäftliche Auswirkungen

Das Projekt führte zu einer umfassenden Umgestaltung sowohl der Sicherheitskontrollen als auch der täglichen Betriebsabläufe.

1. Risikominderung

Das Risiko durch „Shadow IT" wurde durch die Identifizierung und Entfernung nicht autorisierter Anwendungen deutlich verringert. Das Unternehmen erlangte eine stärkere Kontrolle über seine Endgeräteumgebung und reduzierte seine Angriffsfläche insgesamt erheblich.

2. Sichere und kontrollierte Zusammenarbeit

Bisher fragmentierte und auf Vertrauen basierende Prozesse zum Dokumentenaustausch wurden in strukturierte, überprüfbare Arbeitsabläufe mit kontrolliertem Zugriff und Lebenszyklusmanagement umgewandelt. Sensible rechtliche Informationen können nun mit deutlich höherer Sicherheit, Nachvollziehbarkeit und Datenschutz geteilt und verwaltet werden.

3. Transparenz und Nachvollziehbarkeit

Das Unternehmen erlangte vollständige Transparenz sowohl über die Anwendungsnutzung als auch über externe Kooperationsaktivitäten. Datenflüsse wurden nachvollziehbar, Zugriffsereignisse nachprüfbar und die Erstellung von Compliance-Berichten deutlich vereinfacht.

4. Operative Effizienz

Eines der wichtigsten Ergebnisse war die Reduzierung des manuellen Verwaltungsaufwands im Zusammenhang mit der Dokumentenbearbeitung, -verfolgung, dem Scannen und Koordinationsaufgaben.

Verwaltungsteams, die zuvor viel Zeit mit der Verwaltung eingehender und ausgehender juristischer Unterlagen verbracht hatten, konnten diese Prozesse erheblich rationalisieren. Die Organisation sparte Hunderte von Arbeitsstunden ein, reduzierte Prozessengpässe und steigerte ihre Kapazität, wesentlich größere Arbeitslasten ohne zusätzlichen Verwaltungsaufwand zu bewältigen.

5. Benutzererfahrung und Geschäftskontinuität

Trotz der Einführung strengerer Sicherheitsmaßnahmen konnten die Mitarbeiter ihre tägliche Arbeit weiterhin effizient erledigen. Das Projekt schuf einen erfolgreichen Ausgleich zwischen Sicherheit und Benutzerfreundlichkeit und stellte so die Geschäftskontinuität sicher, während gleichzeitig das Schutzniveau verbessert wurde.

Die Rolle von ARMOR360

Als autorisierter Distributor von DriveLock und idgard in Israel fungierte ARMOR360 während des gesamten Projekts als strategischer Implementierungs- und Beratungspartner. ARMOR360 leitete die Initiative von der ersten Bewertung über die Bereitstellung, die Neugestaltung der Prozesse und die Einarbeitung der Nutzer bis hin zur betrieblichen Optimierung.

Zu seinen Aufgaben gehörten:

- **Sicherheitsbewertung und Aufdeckung von Schatten-IT-Risiken**
- **Analyse der Arbeitsabläufe beim Umgang mit rechtlichen Dokumenten**
- **Identifizierung von Sicherheits-, Datenschutz- und Betriebsrisiken**
- **Lösungsarchitektur und -entwurf**
- **Bereitstellung und Konfiguration von DriveLock und idgard**
- **Prozessneugestaltung und Workflow-Optimierung**
- **Einführung der Benutzer und Unterstützung bei der Akzeptanz**

Der Erfolg der Initiative war nicht lediglich das Ergebnis der Einführung der Technologie. Er wurde durch die Integration von Sicherheitskontrollen, Datenschutzanforderungen, Compliance-Zielen und Verbesserungen der betrieblichen Prozesse in eine einheitliche, auf die Bedürfnisse des Unternehmens zugeschnittene Lösung erreicht.

Gesamtergebnis

Das Projekt führte zu messbaren Verbesserungen in den Bereichen Sicherheit, Datenschutz, Compliance und betriebliche Leistung.

Durch die Kombination von DriveLock, idgard und dem Fachwissen von ARMOR360 als autorisiertem Distributor und Implementierungspartner für beide Lösungen in Israel gelang es Geller Han Markovitch, eine Reihe manueller, auf Vertrauen basierender Prozesse in ein kontrolliertes, überprüfbares und effizientes Betriebsmodell umzuwandeln.

Das Ergebnis waren eine höhere Sicherheit, eine verbesserte Durchsetzung des Datenschutzes, geringerer betrieblicher Aufwand, erhebliche Zeitersparnisse, mehr Transparenz und eine reibungslosere Benutzererfahrung sowohl für interne Nutzer als auch für externe Kooperationspartner.

DriveLock idgard®

CASE STUDY

Kundenperspektive

„Das Projekt hat weit mehr als nur stärkere Sicherheitskontrollen gebracht. Es ermöglichte uns, den Datenschutz zu verbessern, vollständige Transparenz und Rechenschaftspflicht im Umgang mit sensiblen Informationen zu schaffen und einen zuvor manuellen und ressourcenintensiven Prozess in einen strukturierten, überprüfbaren und effizienten Arbeitsablauf umzuwandeln. Das Ergebnis waren jährlich eingesparte Hunderte von Verwaltungsarbeitsstunden, erhebliche betriebliche Effizienzsteigerungen und ein wesentlich sichererer und kontrollierterer Umgang mit sensiblen rechtlichen Informationen."

Dieses Projekt ist eine gemeinsame Erfolgsgeschichte von Geller Han Markovitch, DriveLock, idgard und ARMOR360 und zeigt, wie Unternehmen gleichzeitig Sicherheit, Compliance, Datenschutz und betriebliche Effizienz verbessern können, ohne dabei Abstriche bei der Benutzerfreundlichkeit zu machen.

Mit DriveLock und idgard kontrollieren Sie sensible Daten durchgängig – effizient, nachweisbar und souverän.

Sprechen Sie mit unseren Experten

Jetzt unverbindlich 30 Tage gratis testen

Weitere Informationen zu den Produkten von DriveLock und idgard finden Sie unter:

DRIVELOCK.COM | IDGARD.COM