SERVICEWARE

CASE STUDY

WEKO Wohnen stärkt IT-Sicherheit mit CrowdStrike & Serviceware



IT-Sicherheit für einen modernen Möbelhändler

Die WEKO Wohnen Unternehmensgruppe zählt zu den traditionsreichsten Möbelhändlern in Deutschland. Das familiengeführte Unternehmen mit Hauptsitz im niederbayerischen Pfarrkirchen betreibt mehrere Einrichtungshäuser, Fachmärkte und Onlineplattformen wie Garten & Freizeit oder Betten.de. Mit rund 1.000 Mitarbeitenden und einer zunehmend digitalen Geschäftsstrategie stiegen auch die Anforderungen an die IT-Sicherheit deutlich. Gemeinsam mit Serviceware und CrowdStrike modernisierte WEKO deshalb seine Sicherheitsarchitektur.

Das Ziel: Endgeräte besser schützen, den Administrationsaufwand reduzieren und rund um die Uhr auf potenzielle Angriffe reagieren können.



Auf einen Blick

Die Herausforderungen

- Schutz von rund 590 Endgeräten vor Hacker-Angriffen bei begrenzten IT-Ressourcen
- 24/7-Sicherheitsüberwachung intern nicht wirtschaftlich
- Hohe Anforderungen durch hybride Infrastruktur und Onlinehandel

Die Ergebnisse

- Bis zu 80 % weniger Administrationsaufwand
- Managed Security rund um die Uhr mit CrowdStrike Complete
- Nach CrowdStrike-Outage 2024 schon nach wenigen Stunden wieder verkaufsfähig

SERVICEWARE

Der Kunde
WEKO Wohnen

Die Branche
Handel

Das Projekt
Endpoint Protection & Darknet Monitoring mit Crowdstrike – über Serviceware beschafft und beraten

WEKO Wohnen: Tradition trifft E-Commerce und moderne IT

WEKO Wohnen hat sich in den vergangenen Jahren deutlich breiter aufgestellt. Neben den klassischen Möbelhäusern in Pfarrkirchen und Rosenheim gehören heute auch Fachmärkte sowie verschiedene E-Commerce-Plattformen zur Unternehmensgruppe. Besonders mit der Übernahme der Online-Sparte rund um Garten & Freizeit sowie Betten.de gewann die digitale Infrastruktur zunehmend an Bedeutung.

„Da sind Welten aufeinandergeprallt“, beschreibt Stefan Struckmeier, Teamlead IT-Operations und damit verantwortlich für IT-Betrieb und Helpdesk bei WEKO, die Integration der jüngeren Online-Unternehmen in die bestehende IT-Landschaft. Während der stationäre Möbelhandel traditionell gewachsene Prozesse mitbrachte, arbeiteten die Online-Bereiche deutlich agiler und dynamischer.

Die IT-Abteilung wurde in den vergangenen Jahren vollständig zentralisiert und arbeitet heute überwiegend vom Hauptstandort Pfarrkirchen aus. Mit vergleichsweise kleinen Teams verantwortet WEKO den Betrieb zahlreicher Systeme für stationären Handel, Onlineplattformen, ERP, Logistik und interne Prozesse. Gerade deshalb spielt Effizienz in der IT eine zentrale Rolle.

„WEKO war generell schon immer darauf erpicht, dass man alles inhouse managen



kann und wir eigentlich nichts rausgeben“, erklärt Struckmeier. Gleichzeitig wurde aber immer deutlicher, dass insbesondere moderne Cybersecurity-Anforderungen mit eigenen Ressourcen kaum noch wirtschaftlich umzusetzen sind.

Die Komplexität der Handelsprozesse erhöht die Anforderungen zusätzlich. Möbelhandel gilt seit Jahren als besonders individuell – mit zahlreichen Sonderprozessen, spezifischen ERP-Anpassungen und komplexen Vertriebs- und Bonusmodellen. Diese Individualität spiegelt sich auch in den Anforderungen an die IT-Infrastruktur und Sicherheitsarchitektur wider.

Bereits früh setzte WEKO deshalb auf ein mehrschichtiges Sicherheitskonzept mit Rechte- und Rollenkonzepten, Netzwerksegmentierung, Multi-Faktor-Authentifizierung (MFA), VPN-Zugängen und abgesicherten externen Zugriffen über Citrix. Mit zunehmender Bedrohungslage rückte jedoch insbesondere der Schutz der Endgeräte und Benutzeridentitäten stärker in den Fokus.

Die Herausforderung: Warum klassische Antivirus-Lösungen nicht mehr ausreichen

Der Auslöser für die Modernisierung der Sicherheitsarchitektur war zunächst ein ganz praktischer: Die Verträge für die bestehende Antivirus-Lösung liefen aus. Gleichzeitig stellte sich für WEKO die grundsätzliche Frage, wie moderne IT-Sicherheit künftig aussehen sollte.

Auf Fachmessen wie der it-sa beschäftigte sich das Unternehmen intensiv mit verschiedenen Sicherheitsplattformen und verglich Lösungen wie CrowdStrike, SentinelOne und andere Anbieter. Schnell wurde deutlich, dass klassische Virenschutzsysteme den aktuellen Anforderungen nicht mehr gerecht werden: „Eine reine Antivirenlösung war bei uns eigentlich nicht mehr zeitgemäß“, erklärt Struckmeier.

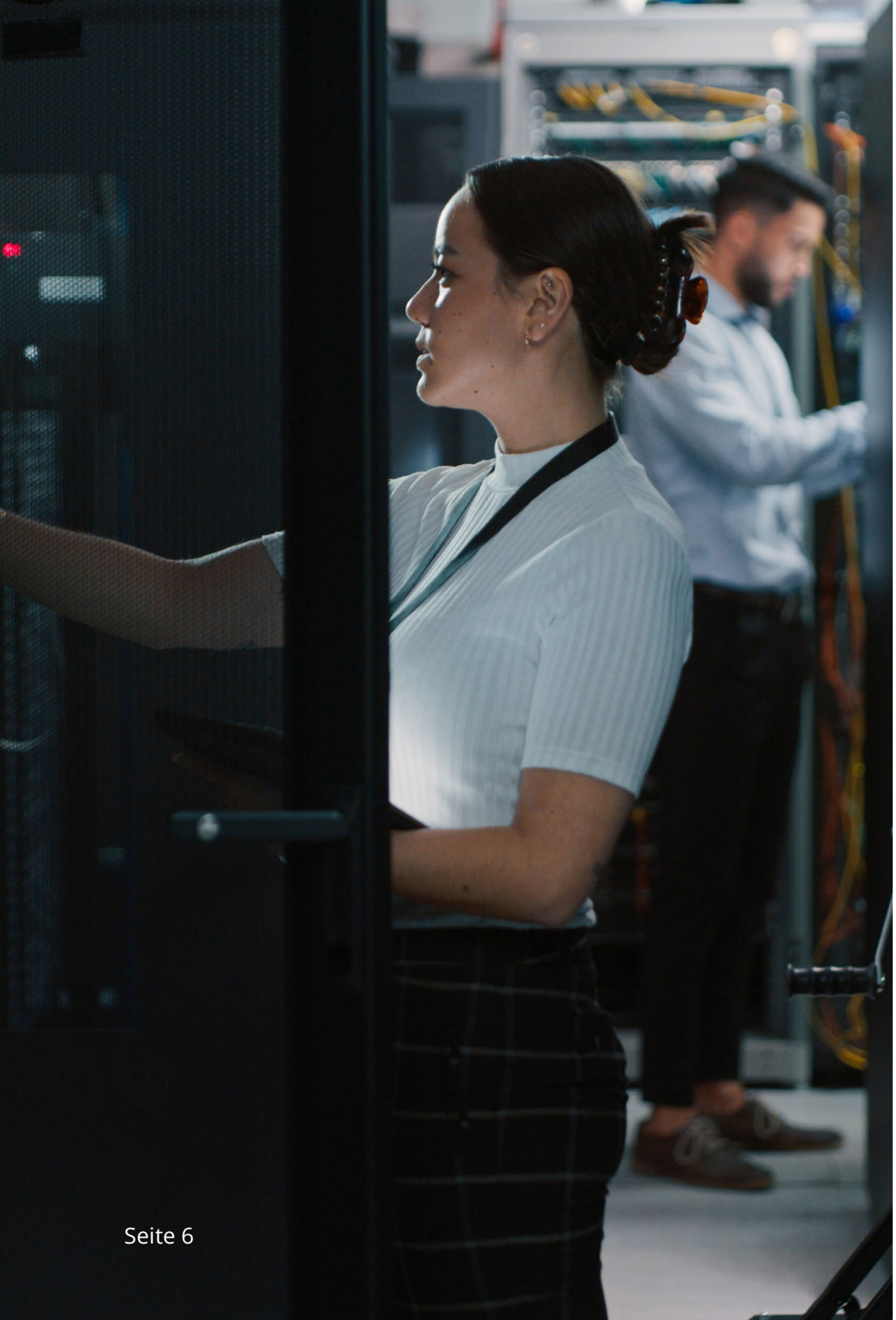
Vor allem das Thema 24/7-Security stellte die interne IT vor große Herausforderungen. Um ein vergleichbares Sicherheitsniveau selbst aufzubauen, hätte WEKO nach eigener Einschätzung mindestens fünf zusätzliche IT-Sicherheitsspezialisten benötigt, inklusive Schichtbetrieb, Urlaubsvertretungen und permanenter Erreichbarkeit.

„Wir haben damals überschlagen, dass uns das intern ungefähr das Fünffache gekostet hätte“, sagt Struckmeier.

Gleichzeitig verschärfte sich die allgemeine Bedrohungslage. Phishing, kompromittierte Benutzerkonten und Ransomware-Angriffe gehörten längst zum Alltag vieler Unternehmen. Auch WEKO war sich dessen bewusst und hatte seine Risikoeinschätzung schon vor der Einführung von CrowdStrike nach oben korrigiert.

Besonders kritisch bewertet WEKO identitätsbasierte Angriffe. Denn moderne Angreifer versuchen häufig nicht den direkten Einbruch in Systeme, sondern bewegen sich mit kompromittierten Benutzerkonten durch die Infrastruktur.

Mit zunehmender Digitalisierung und hybriden Arbeitsmodellen stiegen zudem die Anforderungen an die Endgeräte, an externe Zugriffe sowie die sichere Verwaltung privilegierter Accounts. Gleichzeitig musste die Lösung wirtschaftlich vertretbar bleiben und sich möglichst ressourcenschonend administrieren lassen.



„IT-Sicherheit ist immer ein Thema der vielen Schichten“, beschreibt Struckmeier die Strategie des Unternehmens. „Dank CrowdStrike und der IT-Security-Beratung durch Serviceware können wir nachts beruhigt schlafen, weil wir wissen: Das ganze System ist überwacht und in guten Händen“, betont Struckmeier.

Die Lösung: Managed Detection & Response mit CrowdStrike

Nach einem umfassenden Marktvergleich entschied sich WEKO für CrowdStrike Falcon Complete als Managed Detection and Response (MDR) Plattform. Ausschlaggebend waren dabei sowohl technologische Aspekte als auch die Kombination aus Managed Services und Identity Protection.

Heute schützt CrowdStrike rund 1.200 Identitäten und sämtliche Endgeräte der Unternehmensgruppe – darunter Server, PCs, Notebooks und spezialisierte Systeme.

Zum Einsatz kommen unter anderem:

- CrowdStrike Falcon Complete
- CrowdStrike Identity Protection
- CrowdStrike Device Controll
- 24x7 Managed SOC Services

Besonders wichtig war WEKO die Kombination aus automatisierter Analyse und menschlicher Expertise. „Bei Serviceware und CrowdStrike sitzen wirklich fähige Teams dahinter, die die ganzen Sachen prüfen“, erklärt Struckmeier. „Denn uns war wichtig, dass wenn irgendwo etwas passiert, da jemand



„CrowdStrike ist eine der sichersten Säulen, auf denen unsere gesamte IT-Sicherheitsstrategie heute steht. Im Zusammenspiel mit der Beratung und Betreuung durch Serviceware ergibt sich hier eine echte win-win-Situation“

Stefan Struckmeier
Teamlead IT-Operations,
WEKO Wohnen

mit Menschenverstand draufschaut und pragmatische Lösungen anbietet“, sagt Struckmeier. Ein zentraler Bestandteil der Sicherheitsstrategie ist dabei die Identity Protection. Damit lassen sich Risiken bei Benutzern frühzeitig erkennen, um identitätsbasierte Angriffe aufzudecken und frühzeitig zu stoppen. WEKO nutzt die Lösung nicht nur zur Abwehr der Angriffe, sondern auch zur Optimierung interner Berechtigungskonzepte. „Mit CrowdStrike konnten wir sehr gut nachvollziehen, welche Entwickler tatsächlich auf welche Systeme zugreifen müssen“, beschreibt Struckmeier den praktischen Nutzen.

Als zusätzlichen Schutz setzt WEKO auf CrowdStrike im Bereich der sicheren Nutzung von USB-Schnittstellen auf allen Endgeräten. Das Device Control Modul ermöglicht WEKO die sichere Nutzung externer Geräte, indem USB- und weitere angeschlossene Gerätetypen sichtbar gemacht, überwacht und über granulare Richtlinien kontrolliert werden.

Auch der geringe Betriebsaufwand spielte eine wichtige Rolle. Die ganzheitliche Überwachung der Systeme sowie die Reaktionen auf und Wiederherstellung nach Sicherheitsvorfälle werden weitgehend automatisiert oder direkt durch CrowdStrike übernommen. „Im Vergleich zur alten Antivirus-Lösung brauchen wir vielleicht nur noch ein Drittel oder ein Viertel der Zeit für Wartung und Administration“, so Struckmeier.

CrowdStrike, Serviceware und WEKO performten selbst im Krisenfall

Die Zusammenarbeit mit Serviceware begann ursprünglich über die Suche nach einem erfahrenen CrowdStrike-Partner. Serviceware unterstützte WEKO sowohl bei der Produktauswahl als auch bei Architekturfragen, Konfigurationen und dem laufenden Betrieb. Hinzu kam zudem das finanziell attraktive Angebot, bei dem WEKO bares Geld sparen konnte – bei gleichzeitig verbessertem Sicherheitsniveau.

Aber auch im Ernstfall brachte das gute Zusammenspiel von CrowdStrike und Serviceware einen echten Mehrwert: Denn während des weltweiten CrowdStrike-/Microsoft-BlueScreen-Vorfalls im Juli 2024 arbeitete WEKO eng mit CrowdStrike und Serviceware zusammen. Obwohl nahezu alle Server betroffen waren, gelang es dem Unternehmen innerhalb kürzester Zeit, den Betrieb wiederherzustellen.

„Wir waren trotz des erheblichen Umfangs im Handumdrehen wieder voll verkaufsfähig“, erinnert sich Struckmeier. Serviceware unterstützte dabei unter anderem mit aktuellen Informationen, Handlungsempfehlungen und der Koordination der Wiederherstellungsschritte.

„Auch für den Krisenfall wissen wir also, dass wir uns auf das Zusammenspiel von CrowdStrike und Serviceware immer verlassen können. Wo andere Dienstleister ihre Kunden warten lassen, reagieren sie schnell, professionell und lösungsorientiert,“ so WEKO-Mitarbeiter Stefan Struckmeier.

Stefan Struckmeier
Teamlead IT-Operations, WEKO Wohnen

„Über Serviceware kann ich sagen, dass wir mit der Beratung immer sehr zufrieden waren und sind. Da merkt man, dass wirklich technische Kompetenz beim Serviceware-Team dahinter ist“

Mehr Sicherheit bei weniger Aufwand

Heute sieht sich WEKO im Bereich IT-Sicherheit deutlich besser aufgestellt. Die Kombination aus CrowdStrike Falcon Complete, Identity Protection und der Beratung durch Serviceware hat nicht nur das Sicherheitsniveau erhöht, sondern auch die tägliche Arbeit der IT deutlich vereinfacht.

Ein wesentlicher Vorteil liegt in der permanenten Überwachung der Systeme. Sicherheitsvorfälle werden frühzeitig erkannt und automatisiert gestoppt, bevor größere Schäden entstehen können. „Seit wir CrowdStrike haben, war da zum Glück nichts mehr“, sagt Struckmeier mit Blick auf die IT-Sicherheitslage.

Gleichzeitig reduzierte sich der operative Aufwand für die interne IT erheblich. Gerade für kleinere IT-Teams ist dieser Effizienzgewinn entscheidend. „Jede Minute, die wir uns sparen, ist gern gesehen“, erklärt Struckmeier.

Auch wirtschaftlich erwies sich die Entscheidung somit als sinnvoll. Der Aufbau eines eigenen 24/7-Security-Teams wäre für WEKO personell und finanziell kaum realisierbar gewesen. Gleichzeitig profitiert das Unternehmen heute von der Expertise spezialisierter Sicherheitsteams.

Besonders positiv bewertet WEKO die Zusammenarbeit mit Serviceware: „Serviceware ist für uns in drei Worten zusammengefasst: menschlich, kompetent und lösungsorientiert. Da fühlt man sich als Unternehmen gut aufgehoben“, so Struckmeier.

Heute läuft die Security-Infrastruktur weitgehend automatisiert und stabil im Hintergrund – genau so, wie es sich WEKO vorgestellt hatte. Der Austausch mit CrowdStrike und Serviceware erfolgt vor allem projektbezogen und strategisch: „Wir sind heute der Meinung, dass wir sehr, sehr gut aufgestellt sind“, fasst Struckmeier zusammen.

Sicherheit und Storage aus einer Hand: neben CrowdStrike liefert Serviceware auch Storage-Lösungen von Everpure

Neben der Cybersecurity modernisiert WEKO gemeinsam mit Serviceware auch zentrale Teile seiner Rechenzentrums-Infrastruktur. Zum Einsatz kommt dabei eine FlashArray//X20-R4-Lösung von Everpure (ehemals Pure Storage) mit dem Evergreen//Forever-Modell. Dieses Konzept kombiniert den initialen Hardwarekauf mit laufenden Wartungs-, Upgrade- und Supportleistungen, sodass Controller-Austausch, Software-Updates und Modernisierungen ohne klassische Migrationsprojekte möglich werden.

Stefan Struckmeier
Teamlead IT-Operations, WEKO Wohnen

„Serviceware hebt als Value Added Reseller mit den implementierten CrowdStrike-Lösungen nicht nur unsere IT-Sicherheit auf ein neues Niveau, sondern optimiert auch unser Rechenzentrum um modernste Storage-Lösungen aus dem Hause Everpure.“

Everpure verfolgt dabei einen sogenannten „Always Modern“-Ansatz: Unternehmen sollen ihre Storage-Infrastruktur kontinuierlich modernisieren können, ohne komplette Systeme austauschen oder aufwändige Datenmigrationen durchführen zu müssen. Das Evergreen//Forever-Modell beinhaltet neben proaktiven Support- und Monitoring-Services auch regelmäßige Hardware-Refreshs und flexible Skalierungsmöglichkeiten. Besonders für mittelständische Unternehmen mit langen Investitionszyklen bietet dieser Ansatz eine hohe Planbarkeit bei gleichzeitig moderner Storage-Technologie.

Ziel ist eine langfristig moderne, planbare und wirtschaftlich skalierbare Storage-Architektur mit hoher Verfügbarkeit und geringem Betriebsaufwand. Aktuell prüft WEKO gemeinsam mit Serviceware bereits mögliche Erweiterungen der Plattform – auch vor dem Hintergrund steigender RAM-Preise und wachsender Anforderungen an Performance und Datenvolumen.

Fazit

- Rund 590 Endgeräte werden heute mit CrowdStrike gegen Hacker-Angriffe geschützt
- Bis zu 80 % weniger Administrationsaufwand gegenüber der alten Lösung
- 24/7 Managed Security ohne eigenes Security Operations Center
- Nach dem CrowdStrike-Outage 2024 innerhalb weniger Stunden wieder voll betriebsfähig
- Serviceware begleitet WEKO strategisch, technisch und organisatorisch seit 2023
- Storage-Lösungen von Everpure runden das Serviceware-Angebot bei WEKO sinnvoll ab

Stefan Struckmeier
Teamlead IT-Operations, WEKO Wohnen

Kurzportrait: Stefan Struckmeier, Teamlead IT-Operations, verantwortet bei WEKO Wohnen die Bereiche IT-Betrieb und IT-Helpdesk. Gemeinsam mit seinem Team betreut er die zentrale IT-Infrastruktur der Unternehmensgruppe mit stationärem Handel, E-Commerce und unterschiedlichen Vertriebsgesellschaften. Zu seinen Schwerpunkten gehören IT-Sicherheit, Infrastrukturmanagement sowie die Weiterentwicklung moderner Sicherheitsstrategien.

Über Serviceware

Serviceware bietet seit mehr als 25 Jahren Software, Beratung und Managed Services zur Digitalisierung moderner Unternehmensprozesse. Von Enterprise Service Management über IT Financial Management bis Security, Data und Endpoint Management – hochautomatisiert und sicher.

Serviceware SE
Serviceware-Kreisel 1
65510 Idstein • Germany
+49 6434 9450 0
contact@serviceware-se.com
serviceware-se.com

11/2026

SERVICEWARE