CASE STUDY TOOM BAUMARKT GMBH

toom Baumarkt GmbH: Gesteigerte IT-Basissicherheit schafft Grundlage für besseren Schutz gegen Angriffe

Unterschiedliche IT-Einzellösungen, die einen umfassenden Blick auf den Zustand der Clients erschweren und steigende Anforderungen an die Cyberhygiene: Das waren die Herausforderungen, vor der die toom Baumarkt GmbH Ende 2020 stand. Zur besseren Sicht auf die Umgebung und zur Anhebung der Basissicherheit arbeitet das Unternehmen heute mit den Endpoint Security Services von Magelan, basierend auf Tanium.

Die Herausforderung:

- × Technische Einzellösungen, die nicht miteinander kommunizieren
- × Lückenhafte Sicht auf vorhandene Assets und Anfälligkeiten
- × Keine Möglichkeit, mit bestehenden Lösungen ein umfassendes Schwachstellen-management abzubilden
- × Generelle Anhebung des Basis-Sicherheits-niveaus zur Ausrichtung an den CIS-Controls

Die Lösung:

Magelan Full Managed Endpoint Security Services, basierend auf Tanium

Die Vorteile:

- ✓ Harmonisierung der IT-Landschaft
- ✓ Echtzeittransparenz für das IT-Security Management
- ✓ Verbesserte Visibilität der Assets und Schwachstellen
- ✓ Senkung der Lateral Movement Gefahr durch Betriebssystem-Härtung
- ✓ Reduzierung von Angriffsvektoren durch priorisierte Schließung von Schwachstellen
- ✓ Erhebliche Steigerung der Cyberhygiene

toom Baumarkt GmbH

Branche: Einzelhandel
Teil der REWE Group
Mitarbeiter: rund 18.000
Sitz: Firmenzentrale in Köln

Mit mehr als 300 Märkten im Portfolio (toom Baumarkt, B1 Discount Baumarkt und Klee Gartenfachmarkt), rund 18.000 Beschäftigten und einem Bruttoumsatz von 2,9 Milliarden Euro zählt toom zu den führenden Anbietern der deutschen Baumarktbranche. Das Unternehmen gehört zur REWE Group. Die genossen-schaftliche REWE Group ist einer der führenden Handels- und Touristikkonzerne in Deutschland und Europa. Im Jahr 2021 erzielte das Unternehmen einen Gesamt-außenumsatz von 76,5 Milliarden Euro. Die 1927 gegründete REWE Group ist mit ihren rund 380.000 Beschäftigten in 21 euro-päischen Ländern präsent.
+++ Seit 2016 trägt toom das Zertifikat „audit berufundfamilie“. Mit dem „audit berufundfamilie“, einer Initiative der Gemeinnützigen Hertie-Stiftung, geht toom als Arbeitgeber zukunftsorientierte Wege und unterstützt seine Mitarbeiter in unterschiedlichen Lebensphasen und den damit verbundenen Herausforderungen.

CASE STUDY TOOM BAUMARKT GMBH

Steigende Anforderungen an die Basissicherheit

Die zunehmende Bedrohungslage durch Cyberangriffe zwingt Unternehmen dazu, ihren Blick auf die IT-Basissicherheit zu schärfen. So auch bei der toom Baumarkt GmbH: Im Zuge der Entwicklung einer IT-Security-Strategie entschied sich das Unternehmen für die Ausrichtung an den Standards und Best Practices des Center for Internet Security (CIS Controls). Die CIS Controls bieten eine priorisierte Grundlage von Maßnahmen zur Informationssicherheit, welche kontinuierlich und automatisiert überwacht werden.

Dabei wird im ersten Schritt die sogenannte Cyberhygiene adressiert, d.h. es werden Mindestanforderungen an das grundlegende technische Sicherheitsniveau definiert. Hierzu gehören beispielsweise die vollständige Identifizierung, Inventarisierung und Steuerung von IT-Assets (Hardware & Software) und ein nachweisbares kontinuierliches Schwachstellen- und Patch Management sowie die sichere Grundkonfiguration von Betriebssystemen. Die Automatisierung und permanente Überwachung der Schutzmaßnahmen stehen dabei im Vordergrund.

Das IT-Security-Konzept der toom Baumarkt GmbH wollte genau hier ansetzen. Thorsten Hamers, Information Security Manager, erläutert: „Im Rahmen unserer Strategie hatten wir uns zum Ziel gesetzt, ein breites Niveau an Basissicherheit zu schaffen, von dem aus wir uns kontinuierlich weiterentwickeln können."

> „Das Projekt hat einen erheblichen Anteil daran, dass wir das Basissicherheitsniveau noch einmal grundlegend anheben konnten."
>
> Thorsten Hamers
> Information Security Manager | toom Baumarkt GmbH

Viele Einzellösungen, wenig Visibilität

Das Unternehmen hatte in den Bereichen Endpoint Management und Endpoint Security eine große Zahl individueller Softwarelösungen im Einsatz, die jeweils fachliche Teilanforderungen abdeckten. Es bestand der Wunsch nach einer einheitlichen Sicht auf die Systeme sowie einer besseren Erkennung und Behandlung von Schwachstellen. Wichtigstes Anliegen war es daher, die verteilten Lösungen zusammen zu bringen, um mehr Sichtbarkeit über den tatsächlichen Zustand der IT-Sicherheit zu erlangen und Wissenslücken zu schließen.

Die Lösung: Endpoint Security Services von Magelan basierend auf Tanium

Um diese Herausforderungen zu meistern, entschied sich die toom Baumarkt GmbH für die Full Managed Endpoint Security Services von Magelan, basierend auf der Plattformlösung von Tanium.

Um sicherzustellen, dass Tanium die fachlichen Anforderungen der Speziallösungen abdecken kann, wurden die Funktionen zuvor im Rahmen eines POCs miteinander verglichen – mit einem zufriedenstellenden Ergebnis.

Für toom spielte zudem der Nutzen, der aus der Interaktion von Magelan und Tanium entsteht, eine wesentliche Rolle bei der Entscheidung. Herr Hamers erläutert diesen Mehrwert folgendermaßen: „Es hat sich im Rahmen der Produktevaluation gezeigt, dass das Werkzeug lediglich ein Teil des Gesamterfolgs ist. Für uns bestand der Mehrwert u.a. darin, dass der Output, den Tanium liefert, durch die Managed Services von Magelan verdichtet und vorqualifiziert an die Infrastruktur- und Security-Teams geliefert wird."

In den folgenden Aufgabenbereichen hat sich diese Kombination bereits bewährt:

Asset Discovery

Ganz nach dem Grundsatz „Nur was ich kenne, kann ich schützen" ist verlässliches Asset Discovery ein fundamentales Ziel zur Steigerung der Cyberhygiene. Aufgrund der Managed Services

haben die IT-Abteilung und die IT-Security-Verantwortlichen bei toom inzwischen gute Sichtbarkeit auf die IT-Assets in den einzelnen Baumärkten und auf deren Zustand. Das Wissen, welche Geräte sich im Netz befinden, ob auf jedem Gerät eine Endpoint Protection Lösung installiert ist oder sich beispielsweise Software auf den Geräten befindet, die dort nicht hingehört, ist jetzt umfassend und in Echtzeit verfügbar.

Vulnerability- & Patch Management

Die Endpunkte des Unternehmens werden regelmäßig auf Schwachstellen gescannt und diese mit dem anschließenden Patch & Vulnerability Advisory Service von Magelan priorisiert. Herr Hamers berichtet: „Unsere Anforderung bestand darin, eine vorqualifizierte Ausgabe unserer Schwachstellen zu erhalten, damit wir zielgerichtet und priorisiert patchen können. Durch den Managed Service und das abgestimmte Reporting und Tracking der Veränderungen erreichen wir dies.“ Die Verteilung der Patches lief ursprünglich über ein anderes System, allerdings erwies sich die neue Endpoint Security Plattform auch hier als zuverlässig leistungsstark, so dass nun sowohl das Schwachstellen-Scanning, die Priorisierung von Findings als auch das Patchen mit Tanium erfolgen und ein Systembruch damit vermieden werden kann.

Härtung der Endgeräte

Um die Endgeräte weiter gegen Angriffe zu schützen, will die IT-Security der toom gemeinsam mit Magelan einen industrieweiten Härtungsstandard implementieren und die tatsächlichen Konfigurationen der Geräte automatisiert mit der gewünschten sicheren Konfiguration abgleichen (Configuration Compliance). Hierfür wurden unternehmensspezifische Härtungsstandards auf Basis der CIS Benchmarks für alle eingesetzten Betriebssystemtypen definiert. Diese werden im Rahmen des Service kontinuierlich überprüft und bei Bedarf angepasst.

Visuelle Datenaufbereitung

Themenbezogene automatisierte Security Dashboards mit Live-Daten liefern dem Management einen anschaulichen grafischen Nachweis der Umsetzungserfolge und der IT-Risiken.

Zusammenfassend berichtet Manuel Bolkart, Projekt Manager und Team Lead bei Magelan: „Wir wollen den toom Baumärkten optimale Visibilität und die beste Vorgehensweise liefern, um Schwachstellen priorisiert zu beheben und Endpunkte wiederkehrend zu härten. Damit ist die IT-Basishygiene auf einem sehr guten Level, bietet effektiven Schutz gegen Angriffe und ermöglicht den weiteren Ausbau der IT-Security.“

> „Am Ende des Tages hängt ein Projektverlauf immer an den Menschen und der Zusammenarbeit mit dem Dienstleister. An dieser Stelle ein großes Dankeschön an die Kolleg:innen bei Magelan.“
>
> Thorsten Hamers
> Information Security Manager | toom Baumarkt GmbH

Zufriedenheit in der Zusammenarbeit

Auf die Zusammenarbeit zwischen toom und Magelan angesprochen, sagt Herr Hamers: „Am Ende des Tages hängt ein Projektverlauf immer an den Menschen und der Zusammenarbeit mit dem Dienstleister. An dieser Stelle ein großes Dankeschön an die Kolleg:innen bei Magelan, die sich immer wieder intensiv mit den Anforderungen beschäftigt und das Projekt sehr engagiert gemeinsam mit der toom IT vorangetrieben haben.“

Und weitere Projekte stehen bereits an der Startlinie: So wird gemeinsam mit dem Bereich IT-Operations daran gearbeitet, die Ergebnisse aus dem Asset & IoT Discovery in einer CMDB abzubilden.

Basissicherheit auf einem neuen Level

Ausgehend von dem Ziel, mit IT-Cyberhygiene das grundlegende Sicherheitslevel zu steigern, kann Thorsten Hamers heute zusammenfassen: „Das Projekt hat einen erheblichen Anteil daran, dass wir das Basissicherheitsniveau noch einmal grundlegend anheben konnten.“