VARONIS FALLSTUDIE

Deutsches Maschinenbauunternehmen im Bereich der Serienteilfertigung

DER KUNDE

Deutsches Maschinenbauunternehmen im Bereich Serienteilfertigung

STANDORT

Deutschland

BRANCHE

Maschinenbau, Serienteilfertigung

PRODUKTE

DatAdvantage, DatAlert

„Etwa einen Monat nach der ersten CryptoLocker-Infektion hat es einen weiteren Rechner erwischt. Allerdings hatten wir ja inzwischen DatAlert im Einsatz. Es gelang dem Virus nur etwa 500 Dateien zu verschlüsseln und nicht wie beim ersten Mal 250K. Die Rücksicherung war eine Sache von Minuten und der Aufwand für alle Beteiligten betrug weniger als 15 Minuten.“

GESCHÄFTSANFORDERUNGEN

Berechtigungsmanagement optimieren und mit Analysen des Benutzerverhaltens Datenschutzverstöße erkennen

Sicherheitsaudits sind bei Unternehmen nicht unbedingt beliebt, denn in aller Regel sind sie für das betroffene Unternehmen zeit- und kostenaufwendig. Aber bestimmte Branchen wie beispielsweise der Finanzsektor und in diesem Fall die Automobilbranche setzen sie für Partner zwingend voraus. Bevor die Auditoren ihre Tätigkeit aufnehmen, gilt es schon vorab umfangreiche Fragebögen auszufüllen, die helfen den Sicherheitslevel des Unternehmens zu bewerten. Nicht selten schätzen Unternehmen diesen übrigens deutlich besser ein als er tatsächlich ist.

Vor einigen Jahren wechselte der IT-Leiter eines unserer Kunden von einem Maschinenbauer mit Einzelteilfertigung zu einem Serienteilfertiger. Was ihm besonders positiv auffiel war der hohe Grad an Prozessorientierung. Unumgänglich für einen Serienteilfertiger. Produziert dieser aber auch Teile für den Automobilsektor sind damit bei praktisch allen Konzernen bestimmte Sicherheitsauflagen für die zuliefernden Partner zwingend vorgeschrieben.

DAS ANFORDERUNGSPROFIL

Wie sicher ist sicher? Sicherheitsaudits in der Automobilbranche

Der neue Arbeitgeber unseres IT-Verantwortlichen produziert unter anderem Teile für den Automobilsektor und zwar im Premium-Segment. Vor etwa einem Jahr erreichte den Kunden Post von einem Dienstleister. Dieser sollte im Auftrag eines der besagten Automobilkunden ein Sicherheitsaudit durchführen. Ein entsprechender Fragebogen, der vorab ausgefüllt werden sollte, war gleich dabei.

Wie bei vielen unserer Kunden war die Selbsteinschätzung der Verantwortlichen in Sachen Sicherheit zunächst einigermaßen optimistisch. In diesem Falle ließ sich das auch gut begründen, denn das Unternehmen hatte bereits die BSI-Anforderungen für den Mittelstand zu großen Teilen umgesetzt. Es existierte eine entsprechende IT-Richtlinie, die für alle an PCs arbeitenden Mitarbeiter Geltung hatte und die Bereichsleiter schulten jeden neuen Mitarbeiter noch vor Dienstantritt im Hinblick auf eben diese Richtlinie. Nach Aussagen des IT-Verantwortlichen, der sich um das anstehende Sicherheitsaudit kümmern sollte, rechnete er selbst mit einer Erfüllungsquote von etwa 70-80 %.

DEUTLICH DARUNTER...

Wer schon ein Mal selbst mit Audits dieser Art in Berührung gekommen ist, insbesondere mit solchen wie sie in der Automobilbranche üblich sind, der weiß in etwa, was auf ihn zukommt. Der Fragebogen beinhaltete mehr als 50 verschiedene Fragen aus unterschiedlichen Gebieten der Informationssicherheit, die mit einer 6 Stufen umfassenden Skala bewertet werden konnten. Der Zielreifegrad ist die Stufe 4, sozusagen die „Pflicht“, alles darüber Kür.

Die Bewertung nach der Beantwortung der ersten Frage fiel für unseren Kunden noch positiv aus. Allerdings reichte es schon bei der zweiten Frage nur noch für Stufe 2 und die weitere Beantwortung fiel nicht wesentlich besser aus. Nach eigenen Angaben erreichte das Unternehmen unseres Kunden nach einer ehrlichen Bestandsaufnahme des Sicherheitslevels im Unternehmen lediglich 58 % im Hinblick auf die Vorgaben. Das war natürlich deutlich zu wenig.

Als unmittelbare Konsequenz und nachdem das Thema der Geschäftsleitung vorgestellt worden war, wurde ein Team gebildet, das einen vorläufigen Maßnahmenkatalog erstellen sollte. Es setzte sich aus Mitarbeitern der prozessbetroffenen Bereiche, den Qualitätsmanagement-Beauftragten, dem Leiter der IT-Abteilung sowie Mitarbeitern aus der IT zusammen.

WARUM VARONIS?

Weniger Aufwand und mehr Sicherheit?

Schon während das eigens zusammengestellte Team den Maßnahmenplan ausarbeitete, wurde geprüft, ob und wenn ja, an welchen Stellen verschiedene Tools helfen könnten die eigentlichen Umsetzungszeiten zu verkürzen. Aus Sicht der IT-Abteilung kristallisierten sich zwei Bereiche heraus, in denen mehr Aufwand erforderlich werden würde: Der Bereich Patch-Management und vor allem das Überprüfen und Bewerten der Zugriffsberechtigungen auf Daten. Ein Bereich, in dem sich noch dazu der Mehraufwand schwer beziffern ließ. Schließlich würde man zunächst ein Mal sämtliche Daten qualifizieren und als öffentlich, normal, vertraulich und geheim bewerten müssen. Anschließend würde man für jeden dieser Bereiche überprüfen müssen, ob die Zugriffsberechtigungen korrekt vergeben worden sind, ob sie noch aktuell sind und nur genau die Personen darauf zugreifen können, die tatsächlich dazu berechtigt sind.

Wer schon ein Mal versucht hat eine solche Aufstellung mit Bordmitteln umzusetzen, der weiß wie immens zeitaufwändig dieses Vorgehen ist; die manuelle Vorgehensweise birgt zudem noch eine ganz Reihe potenzieller Fehlerquellen. Ohne eine logische oder geeignete Berechtigungsstruktur ist es nahezu unmöglich, zu identifizieren, wer mit den Daten arbeitet und welcher Abteilung diese Daten gehören. Geschweige denn lässt sich sicherstellen, dass nur die richtigen Abteilungen und Personen Zugriff auf die entsprechenden Daten haben.

ZUGRIFFSVERWALTUNG UND BERECHTIGUNGSMANAGEMENT OPTIMIEREN

Der Zufall wollte es, dass just zu diesem Zeitpunkt ein Webinar mit Varonis geplant war, in dem das Unternehmen seine Lösung vorstellen wollte. Die Lösungen stellt sicher, dass nur die richtigen Benutzer Zugriff auf die richtigen Daten haben, und dass der Zugriff überwacht und Missbrauch angezeigt wird.

So lässt sich zum Beispiel analysieren welche Gruppen und Personen auf gewisse Daten zugreifen können und welche dieser Personen den Zugriff auch tatsächlich nutzen. Dazu kommen automatisch generierte Reports, die man in regelmäßigen Abständen erstellen und versenden lassen kann. Aufgrund dieser Berichte ist der zuständige Bereichsleiter in der Lage zu überprüfen, wer auf welche Informationen zugreifen kann. Das war beispielsweise einer der wichtigen Punkte im Audit-Fragebogen. Das Sicherheitsaudit bestätigte schließlich die vorherige Selbsteinschätzung des Unternehmens, so dass der Maßnahmenkatalog frei gegeben und die mit den einzelnen Maßnahmen assoziierten Produkte bestellt wurden.

Das Unternehmen orderte DatAdvantage und DataAlert. Datadvantage protokolliert und analysiert die Datenzugriffe und Berechtigungen. Datalert wiederum ist ein kleines Tool, das aktiv auf den Fileservern gewisse Verhaltensmuster überwacht. Kommt es zu Abweichungen von den vorher als Regelfall definierten Mustern, gibt es einen Alert aus und ist zusätzlich in der Lage selbständig bestimmte Aktionen auszuführen.

- Mit DatAdvantage kann ein Unternehmen die Aktivitäten der Benutzer nachverfolgen und die Zugriffe auf Dateien überwachen. Das Benutzerverhalten wird mit Hilfe lernender Algorithmen ausgewertet und Berichte zu allen Aktivitäten auf den Fileservern erstellt.
- Parallel werden die tatsächlichen Dateneigentümer identifiziert und können anschließend in die inhaltlich richtige Vergabe von Zugriffsberechtigungen involviert werden. Gleichzeitig werden Meldungen und Berichte so ausgegeben, dass Compliance-Anforderungen erfüllt werden.
- Varonis DatAdvantage kombiniert Benutzer- und Gruppeninformationen mit den Berechtigungsmetadaten aus den Fileshares, um die Zugriffsstruktur des Unternehmens vollständig abzubilden. Diese Informationen werden anschließend mit der Zugriffsaktivität und Benutzerverhaltensanalysen kombiniert, um automatisch Benutzer und Gruppen zu finden, die inaktiv oder überflüssig sind. In den solcherart hervorgehobenen Bereichen kann man Berechtigungen dann sicher entfernen. So lassen sich Probleme beheben, Risiken senken und Fragen dazu beantworten, wer auf Daten zugreifen kann und sollte – entscheidende Fragen im Zuliefersektor der Automobilindustrie.

RESULTATE

CryptoLocker und die Folgen—Ransomware erkennen, Schaden minimieren

Unser Kunde installierte zunächst die Lösung für das Zugriffs- und Berechtigungsmanagement. Die Funktionen von DatAlert wollte die IT-Abteilung erst noch testen. So blieb DatAlert zunächst noch inaktiv, was sich in der Folge als einigermaßen fatal erwies.

Der IT-Leiter unseres Kunden: „Diese Entscheidung ist uns etwa eine Woche nachdem wir DatAdvantage installiert hatten, beinahe zum Verhängnis geworden. Auf einem unserer Client-PCs war die Ransomware CryptoLocker aktiv und wurde erst nach mehreren Stunden entdeckt und gestoppt. Dank DatAdvantage konnten wir die betroffenen Bereiche allerdings sehr schnell ermitteln und sofort mit der Rücksicherung beginnen. Nach dieser Erfahrung haben wir DatAlert sofort scharf geschaltet. Mit einem zusätzlichen PowerShell-Skript ist es jetzt sogar möglich, dass bei einem entsprechenden Alert sofort die Berechtigungen entzogen werden."

Innerhalb von DatAlert kann der Benutzer in Bezug auf Änderungen an Konfigurationsdateien, Events oder Änderungen, die außerhalb der dafür bestimmten Kontrollfenster stattfinden, Regeln setzen und die Filter folgendermaßen konfigurieren:

- Wer – aktives Objekt (Benutzer, Gruppe)
- Wo – betroffenes Objekt (Ordner, Gruppe)
- Was – Details des Aktion (Event-Typ)
- Wann – Zeitfenster

und in welcher Form benachrichtigt werden soll.

Die populäre Ransomware Cryptolocker verwendet bestimmte Aktionen und Strukturen, die sich in bestimmten Dateiereignissen wiederspiegeln. Das sind zum Beispiel Aktionen wie das Öffnen, das Umbenennen und Anlegen von Dateien auf dem Fileserver. Dazu kann ein Unternehmen in DatAlert die Benachrichtigungen so konfigurieren, dass sie beim Überschreiten bestimmter Grenzwerte für diese Aktionen einen Alarm auslösen. Man kann die Benachrichtigungen auch auf der Basis einzelner Dateien konfigurieren, um zu erkennen, wenn „Ransom Note“-Dateien angelegt worden sind. Zusätzlich lassen sich automatisch ablaufende Aktionen einstellen, um Anzeichen einer potenziell erfolgten Infektion zu überprüfen und gegebenenfalls AD-Kontos zu deaktivieren. Die Datei-Verschlüsselung befindet sich dann in einer Quarantäne und kann sich nicht weiter verbreiten.

FAZIT

Mehr Sicherheit, weniger Aufwand und ein anderer Blick auf die IT-Sicherheit im Unternehmen

Der Leiter der IT-Abteilung noch ein Mal abschließend: „Etwa einen Monat nach der ersten CryptoLocker-Infektion hat es einen weiteren Rechner erwischt. Allerdings hatten wir ja inzwischen DatAlert im Einsatz. Es gelang dem Virus nur etwa 500 Dateien zu verschlüsseln und nicht wie beim ersten Mal 250K. Die Rücksicherung war eine Sache von Minuten und der Aufwand für alle Beteiligten betrug weniger als 15 Minuten. Im Moment befinden wir uns beim Umsetzen des Maßnahmenkataloges in der abschließenden Phase werden das Team aber nach dem Abschluss weiterhin am Thema arbeiten lassen. Wir werden uns dabei an der ISO 27001 orientieren, um die Prozesse und Richtlinien der Firma in einem PDCA-Zyklus weiter zu optimieren. Das Sicherheits-Audit hat unserer Firma gut getan. Denn es hat unsere Sichtweise grundlegend verändert und den Fokus unserer Aktivitäten wie beschrieben verändert. Was die IT-Sicherheit anbelangt sind wir jetzt bei weitem besser aufgestellt als vor dem Audit und aufgrund der verwendeten Tools hat sich der Mehraufwand in Grenzen gehalten.“

ÜBER VARONIS

Varonis ist ein führender Anbieter von Software-Lösungen für unstrukturierte, manuell generierte Unternehmensdaten. Varonis bietet eine innovative Software- Plattform, mit der Unternehmen ihre unstrukturierten Daten abbilden, analysieren, verwalten und migrieren können. Wir konzentrieren uns auf manuell generierte Daten, eine Art der unstrukturierten Daten, die Tabellen, Textverarbeitungsdateien, Präsentationen, Audio- und Video-Dateien, E-Mails, Textmitteilungen und alle anderen durch Mitarbeiter erstellten Daten umfassen. Diese Daten enthalten häufig betriebliche Finanzinformationen, Produktpläne, strategische Initiativen, geistiges Eigentum und zahlreiche andere Formen unentbehrlicher Informationen. IT- und Business-Personal nutzen die Varonis-Software für verschiedenste Anwendungsfälle, einschließlich von Data Governance, Datenschutz, Archivierung, Dateisynchronisation, verbesserte mobile Datenverfügbarkeit und Informationsaustausch.

30 Tage kostenlos testen:

INNERHALB DER ERSTEN STUNDEN NACH DER INSTALLATION

Sie können sofort Berechtigungsprüfungen durchführen: Zugriffsberechtigungen für Ordner und Dateien und wie sich diese zu bestimmten Benutzern und Gruppen abbilden lassen. Sie können sogar bereits Berichte erstellen.

INNERHALB VON EINEM TAG NACH DER INSTALLATION

Varonis DatAdvantage beginnt Ihnen die Arten und Benutzer von Zugriffsberechtigungen aufzuzeigen.

INNERHALB VON 3 WOCHEN NACH DER INSTALLATION

Varonis DatAdvantage wird zuverlässige Empfehlungen dazu erstellen, wie Zugriff auf Dateien und Ordner beschränkt werden kann, sodass nur die richtigen Personen Zugriff darauf haben.

KOSTENLOSEN TEST JETZT STARTEN