IHS [導入事例]

サーバーセキュリティパッチ適用作業の運用設計・環境構築

背景

プライベートクラウド、オンプレミスなど、サーバーの形態を問わず、システム構築時には企業・組織の規模や特性によって一定水準以上のセキュリティ対策を検討し、構築されることと思います。
しかしながら、構築時に強固なセキュアシステムを構築していても、システムで利用されているサービスに、新たな脆弱性が発見されてしまうことにより、一転して脆弱なシステムとなり、セキュリティ上の脅威に晒されてしまう結果となってしまいます。
2017 年上半期には「 WannaCry 」と「 Petya 」という 2 種のランサムウェアによる世界的な被害も話題になりました。
このような後発的なセキュリティの脆弱性への対策として、システムで利用している OS やサービスに関連する最新セキュリティ情報収集を継続的に行い、対象システムの脆弱性情報が報告された場合は、すみやかに実施可能なポリシーを構築することが大切であり、お客様の課題でもありました。

概要

業種	小売業
目的	サーバーセキュリティパッチ適用作業の運用設計・環境構築
作業ボリューム	10 人月
作業内容	• 現状調査・整理 • セキュリティパッチ適用の要件定義 • 要件定義後の後続作業の計画作成 • セキュリティパッチの運用設計 • セキュリティパッチの適用環境構築 • 全サーバー別の作業手順書作成・評価 • 運用設計に沿った検証環境への適用 • 運用設計に沿った本番環境への適用

セキュリティパッチ適用の運用設計により得られる効果

- 緊急対応が必要になった際も、決められたプロセス、手順により素早く対応が可能
- 定期的なセキュリティパッチ適用作業を運用に組み込むことにより、セキュリティの維持管理を実現

弊社利用による効果

- これまで弊社が、数社のシステム運用支援で培ったセキュリティパッチ適用に必要なプロセス管理手法（サービスの停止方法・適用方法・作業後の正常性確認・想定外の事象発生時の事前対策等）を基に、お客様の利用形態と照らし合わせてより安全な手法で効率的にパッチ適用が実施できるように最適な運用設計をご提案するに至った。

- 対象となる業務サーバーのパッチ適用による影響度などを運用開始前に調査した上で、適用頻度や手法、適用後の動作確認方法などを決定したことから、適用作業による障害等の発生リスクを抑える事が可能となった。

作業効果

＜課題の詳細＞

- セキュリティパッチ適用の運用方式がない。
- 属人的にシステムが管理されており、毎回各システム担当者へセキュリティパッチの調査/影響度/手順書の準備などが発生するため、多大な時間がかかり、負荷が高い。
- 運用チームは存在するが、人的リソースが不足している。

＜どのように改善したか＞

- セキュリティパッチを適用することを前提とした運用の設計を構築。
- システム毎にセキュリティパッチの適用方式、適用手順を作成。
- 弊社にてセキュリティパッチ適用時の運用を実施。

＜どのような効果があったか＞

- 運用方法を明文化することにより、セキュリティパッチの適用要否を判別/適用対象サーバーの基準が明確化され、定期的なセキュリティパッチを適用する運用が可能になった。
- 属人的に管理されていたサーバー停止可能時間、サーバー起動・停止方法を一覧表でまとめて管理し、明確になった。
- 緊急度が高く、すべてのサーバーへ対処が必要になった場合でも定義された作業プロセスと作業手順により対応が可能となった。
- 複数のシステム（サーバー数は約 250 台）が稼働しているが、それぞれの環境やシステムに合わせた作業プロセスが整理され、明文化されたことで、属人化を排除し、環境の有識者のみが対応可能な状況を排除することができた。
- 弊社にて定期的に情報処理推進機構（ IPA ）及び、各ベンダーによるセキュリティ情報（脅威の内容、対象環境）を確認、および報告をすることで、脅威に対する対策方法、判断材料が提供されるようになり、運用チームの負担が軽減された。
- 弊社にてセキュリティパッチ適用の準備、および作業を実施するため、運用チームの負担が軽減された。

作業内容の詳細

現状調査

1. システム環境・運用状況の調査
2. 対象システム・対象サービスの整理
3. 現状の作業プロセス、手順の確認、整理
4. システムバックアップ実装の有無調査

セキュリティパッチ適用の要件定義

1. 現状分析
2. ユーザーヒアリング
3. 要件定義書作成

要件定義後の後続作業の計画作成

1. WBS 作成

セキュリティパッチの運用設計

1. ユーザーヒアリング
2. 基本設計書作成
3. 詳細設計書作成
4. 運用設計書作成

セキュリティパッチの適用環境構築

1. WSUS 構築
2. グループポリシー設定

全サーバー別の作業手順書作成、評価

1. 各サーバーの手順書を作成
2. 作成した手順書の評価、机上テストを実施

運用設計に沿った検証環境への適用

1. セキュリティパッチの情報収集、パッチ一覧表作成
2. パッチ適用、適用後の動作確認

運用設計に沿った本番環境への適用

1. 検証環境の適用結果確認
2. パッチ適用、適用後の動作確認

IHS IIMヒューマン・ソリューション株式会社
〒113-0033 東京都文京区本郷2丁目27番20号 本郷センタービル6F
TEL : 03-5684-6840(代) FAX: 03-5684-6776
E-MAIL : ihsinfo@iimhs.co.jp
URL : http://www.iimhs.co.jp/