Woodland Academy

情報セキュリティ演習

演習問題

Shape Your Future

GitHub上へのソースコード流出事案　時間：　30　分

事例：三井住友銀行システムのソースコード流出問題

2021年1月28日、三井住友銀行（SMBC）が使用しているシステムのソースコードが公開・流出した可能性がSNSで指摘されました。翌29日、SMBCは指摘されたコードが自社の行内システムの一部と一致することを確認しました。この問題は、NTTデータの子会社であるNTTデータ ジェトロニクスを含む複数の関連企業にも影響が及び、被害の公表が相次ぎました。

- 上記の事例について、発生した原因、起こりうるリスク、再発防止策を検討してください。

Woodland Academy

GitHub上へのソースコード流出　時間：　　分事案

＜発生原因＞

1.情報重大性への理解不足

1.当該エンジニアが、業務で取り扱うソースコードの重要性や守秘義務について十分な理解をしていなかった。

2.ソースコードが「公開設定」であることを認識していなかった、または軽視していた。

2.ツール利用時の設定ミス

1.GitHubの公開/非公開設定について適切に把握していなかった。

2.外部サービス利用時の安全性や公開リスクを考慮せず、情報を外部に提供していた。

3.組織的な管理不備

1.リモートワーク環境の増加による情報管理体制の不備。

2.多重下請構造の影響で、末端エンジニアまで情報管理の徹底が行き届いていない。

4.教育・指導の不足

1.セキュリティリテラシー向上を目的とした教育・研修が不足していた。

Woodland Academy

GitHub上へのソースコード流出　時間：　　分事案

<起こりうるリスク>

1.直接的なリスク

1.ソースコードが公開されることで、システムの脆弱性を突かれる可能性がある。

2.セキュリティ侵害や不正アクセスによる追加被害の発生。

2.法的リスク

1.不正競争防止法や著作権法への抵触。

2.守秘義務違反や不法行為責任の追及。

3.エンドユーザや元請けからの損害賠償請求。

3.信用失墜

1.発注元や最終エンドユーザ企業の社会的信用の低下。

2.利用者からの不信感による顧客離れ。

4.クラウドサービスの活用制限

1.GitHubなどのツール利用に対する萎縮が生じ、生産性が低下する。

Woodland Academy

GitHub上へのソースコード流出　時間：　　分
事案

＜再発防止策＞

1.教育・啓発

1.業務上取り扱う情報の重大性に関する教育を実施。
2.GitHubなどのツールの利用方法やリスクについて、定期的な研修を行う。

2.情報管理体制の強化

1.リモートワーク環境でも対応可能なセキュリティポリシーを構築。
2.情報の公開範囲設定やデータ保存ルールの明確化。
3.多重下請け構造における管理責任の明確化と契約条件の見直し。

3.ツール利用ガイドラインの整備

1.GitHubなどのクラウドツール利用における設定マニュアルを作成。

4.迅速な対応体制の構築

1.インシデント発生時の対応手順を整備。
2.迅速な事実確認と公表、再発防止策の提示を行う体制を確立。

Woodland Academy

患者情報の紛失事案　　時間：　30　分

事例：横浜市立みなと赤十字病院における患者情報の紛失問題

横浜市立みなと赤十字病院（以下「みなと赤十字病院」）の医師が、論文作成のために患者の個人情報を保存したUSBメモリを院外に持ち出し、その後紛失しました。このUSBメモリには患者の氏名、診療記録、その他個人を特定できる情報が含まれていたとされています。情報の持ち出し方法や管理体制に不備があった可能性が指摘されています。

- 上記の事例について、発生した原因、起こりうるリスク、再発防止策を検討してください。

Woodland Academy

患者情報の紛失事案　　時間：　　分

＜発生原因＞

1.管理体制の不備

1.USBメモリによる情報持ち出しが、適切な承認や記録なしに行われていた可能性。

2.持ち出し用のUSBメモリに暗号化などのセキュリティ対策が施されていなかった。

2.教育不足

1.医師や職員に対する情報セキュリティ意識が十分に醸成されていなかった。

2.個人情報保護に関するルールやリスクの周知が不十分だった。

3.運用ルールの形骸化

1.持ち出しに関する運用ルールが存在しても、実効性のある運用がなされていなかった。

Woodland Academy

患者情報の紛失事案　　時間：　　分

<起こりうるリスク>

1.患者への影響

1.個人情報が第三者に流出した場合、不正利用やプライバシー侵害が発生する可能性がある。

2.患者の信頼喪失による病院の評判低下。

2.法的リスク

1.個人情報保護法違反により、行政指導や罰金などの法的措置を受ける可能性。

2.損害賠償請求による経済的損失。

3.運営上のリスク

1.信用失墜による患者数減少や採用への悪影響。

2.病院全体でのセキュリティ対応コスト増加。

Woodland Academy

患者情報の紛失事案　　時間：　　分

＜再発防止策＞

1.技術的対策

1.情報を保存するデバイスには、必ず暗号化やパスワード保護を施す。

2.USBメモリの使用を制限し、クラウドやVPNを活用した安全な情報共有を推奨する。

2.運用上の改善

1.持ち出しが必要な場合、事前承認や記録を義務付ける運用ルールの明確化。

2.データ持ち出し後の返却確認を徹底。

3.教育・研修の強化

1.医師や職員向けに、定期的な情報セキュリティ研修を実施。

2.実際の事例をもとに、リスクや重要性を理解させる教育を行う。

4.監査体制の強化

1.情報管理のルールが守られているか定期的に監査する仕組みを構築。

2.個人情報の取り扱いに関するトレーサビリティ（追跡可能性）の確保。

Woodland Academy

フィッシング詐欺による機密情報の窃取事案

時間：　30　分

事例：フィッシングメールによる不正アクセス被害

金融機関の社員が「システムメンテナンスのお知らせ」と題されたメールを受信。このメールはフィッシングメールであり、社員は文面を信じてメール内のリンクをクリックし、偽のログインページにパスワードを入力してしまいました。その結果、第三者にログイン情報が盗まれ、不正アクセスによって複数の顧客口座から資金が引き出される被害が発生しました。

- 上記の事例について、発生した原因、起こりうるリスク、再発防止策を検討してください。

Woodland Academy

フィッシング詐欺による機密情報の窃取事案

時間：　　分

＜発生原因＞

1. **フィッシングメールの見極めができなかった**
   1. 社員がメールの正当性を十分に確認せず、リンクをクリックした。
   2. メールの差出人や内容の信頼性を確認する意識が不足していた。
2. **セキュリティ意識の欠如**
   1. 「システムメンテナンス」という一見正当な内容に対して、疑念を抱かず行動した。
   2. 不審なリンクや偽サイトに関する知識が不足していた。
3. **多要素認証の不備**
   1. 不正ログインのリスクを軽減するための多要素認証が適切に設定されていなかった。

Woodland Academy

フィッシング詐欺による機密情報の窃取事案

時間：　　分

<起こりうるリスク>

1.顧客資産の損失

1.不正アクセスによる資金の引き出しや口座情報の流出。

2.信頼の毀損

1.顧客からの信頼が低下し、金融機関としての信用が損なわれる。

3.法的・経済的リスク

1.被害補償や法的対応に伴う多大なコストが発生する可能性。

4.さらなる攻撃のリスク

1.他のシステムや顧客口座への攻撃が拡大する恐れ。

Woodland Academy

フィッシング詐欺による機密情報の窃取事案

時間：　　分

＜再発防止策＞

1.フィッシング対策の強化

1.定期的な情報セキュリティ研修を実施し、フィッシングメールの特徴や注意点を周知。

2.不審なメールへの対応フロー（差出人確認、リンク未クリックなど）を徹底。

2.多要素認証の導入

1.ログイン時にパスワードだけでなく、ワンタイムパスコードや生体認証を活用する仕組みを導入。

3.システム面での防御強化

1.フィッシングメールを自動検知・隔離するメールフィルタリングシステムの導入。

4.インシデント対応体制の整備

1.不正アクセスや情報漏洩が発生した際の迅速な対応手順を策定。

2.被害を最小限に抑えるための緊急対応訓練を実施。

Woodland Academy