ゼロトラストにおけるファイル共有のあり方

クラウド生活のすすめ

株式会社プロキューブ

ゼロは思考停止？

- ゼロリスク、バグゼロ、ゼロコロナ
  - インシデント、バグ、感染のリスクについて、絶滅を目指して発生確率も被害額も何も考えずにとにかくやれることをやる→**美しき思考停止**
  - 日本人は「完璧を目指してやれることはすべてやる」・「民度の高さで勝負」が好き→ITの世界では変化が激しく完璧を達成できない→**日本のIT業界の弱点**
- ゼロトラストでは、ネットワーク、サーバ、端末、ソフトウェア、ユーザの何も信用しない＝完璧は無理→インシデント、バグについて一つ一つ吟味・選別（＝リスクアセスメント＝トリアージ）して効率を上げて対応するしか無い→ゼロリスクとは反対の考え方
  - リスクの期待値（＝被害額×発生確率）を**見積もる**必要がある
  - 今リスク期待値の高そうなのって何？→WordとExcel の**ファイル**です

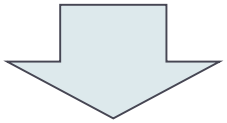
レベル０：NAS

- バッファロー/IODATAのNASをネットワークに接続しただけの状態だけど、インターネットからは入れないネットワークだから大丈夫
- ログイン不要でサクサク
- RAID1だから安心

- 今やVPN装置の脆弱性が原因で閉域網に侵入されるケース（半田病院事例）もあり、閉域網の神話を信じてはならない
- 外部の業者やアルバイトのパソコンから侵入する場合もあり、ユーザやデバイスに対する性善説は危険
- RAID1でもディスクは故障したら交換する必要があるので、故障を検知できる運用が必要
- Wifiで部外者が勝手にアクセス
- NASにユーザ登録して認証機能を利用するのは運用負荷が高すぎてできない
- 全社としてはADが導入されてIDが管理されていても、部門で勝手にポチったNASが置いてある場合がある

レベル1：Active Directory

- Active Directory に登録されたコンピュータとユーザしかアクセスさせないから安心



- やっぱりユーザとデバイスを信用してしまうとセキュリティリスクが生じる（https://mnb.macnica.co.jp/2022/10/AD.html がよくまとまっているので、これで説明する）境界型防御は効かない
- PPAPでパスワード付きZIPファイルをダウンロードすると展開するまで中身のスキャンはできない→PPAPやめよう
- Windows ファイル共有（SMBプロトコル）の暗号化はデフォルトではオフなので、ネットワーク内でパケットキャプチャするだけでファイルの内容は丸見え
- ID管理・各種設定について
  - 退職者のアカウントがいつまでも有効なまま残っている→アカウントの有効期限を設定して、継続申請などのワークフローを運用する
  - 共用アカウントを使用している→ただちにやめて、グループによる認可に切り替えるべき＝3日しか働かないアルバイトであっても個別にアカウントを払い出すべき
  - 従業員数が100人を超えるとA/DのUIですべてを管理するのは無理→ID管理システムが必要（組織ごとのセキュリティグループや役職単位のセキュリティグループを持ちながら年次人事異動ができること）

最小権限の原則

- ファイルサーバでウイルス感染、情報漏えい等のインシデントが発生した場合でもファイルごとにアクセスできる人を最小限にしておけば被害を最小化できる
- 特権ユーザのアクセスは特に厳しいアクセス制御が必要
- アクセス制御には拒否、許容以外に以下が考えられる
  - 監査通知：アクセスをリソースのオーナーに通知する
  - オンデマンド許可：アクセスが必要となったときにワークフローでリソースのオーナーから許可を得る
- ユーザのアカウントに有効期限をつけて、定期的に棚卸しするのが効果的
- **そもそもゼロリスクを目指すのではなく、リスクの最小化を目指すべき**

レベル2: クラウドファイル共有

- Google共有ドライブ、OneDrive、Boxなどのクラウド上ファイル共有を利用
- 編集するときはファイルをダウンロードして編集
- 最小権限の原則に従って、ID、グループを作成し、適宜アクセス権を付与する

- できれば、ダウンロードせずに編集できる方がよい
  - Googleスプレッドシートや Officeオンラインを使用する
  - SharePointのローカルアプリで編集する機能を使用する

アクセス制御はユースケース単位で

- ファイル共有で仕事をするときのユースケースは新規作成、閲覧、更新、削除くらいの分類しかできない
- しかし、実際にはユースケースがいろいろあり、ユーザの役割に従って制御される必要がある
  - 稟議書の承認
  - 注文、発注
  - 文書のドラフト作成、改版、承認
  - 外部への開示
- 結局ファイル共有では権限の最小化の原則を満たせない

レベル3: Webデスクトップ（ローカルファイルなし）

- VDI不要だし、性能を確保するのが難しいVDIよりは使いやすいんじゃない？
- キャッシュには残るけど、そこはディスク暗号化を信用しよう。
- どうせネットワーク切れてたら仕事なんてできないし、 HTML5 local storage ならネットワーク切れてても使えるし。
- もうすぐ http3 の時代になって、ますますクラウド依存度が高くなる
- ローコード/ノーコード系のWebアプリフレームワークでDX。
- FIDO 二要素認証で本人確認の精度向上
- セキュリティの技術は常に最新のものを利用可能

Webデスクトップアプリ

- CMSをグループウェア代わりに
  - lumapps
- 開発系
  - harファイル解析
  - Typescript playground
  - JWT解析
  - unix時間などの計算
- CRM
  - Misoca
  - vTiger
- Google workspace
  - カレンダー
  - ToDoリスト
  - 連絡帳

ファイル共有の制御を自動化

- ファイルが外から送られてきてしまうので Webデスクトップはまだできない
- 組織ごとのセキュリティグループや役職単位のセキュリティグループを持ちながら年次人事異動ができること
- ポリシーを作成するのは工数は必要だけど、ファイル単位に設定するよりは安全
- ID管理ソフト infoScoop ID Managerでできるものもある
- Skyhigh CASB で実装可能
- Microsoft Automatic Labeling