ここが変だよ、日本のセキュリティ
～対策の光と影～

@ AVTOKYO2013.5

愛奴 & 愛花

翻訳協力：米澤一樹

Agenda

- 背景
- メール添付ファイルの暗号化
- ログ統合監視による内部不正検知
- データセンターでの手荷物検査
- 最新のインテリジェンスビル
- IDカードによる入退室管理
- まとめ

背景

- セキュリティ対策の導入には、利便性や費用を犠牲にする側面があります
- しかし、そうした犠牲が必ずしも報われないケースがあります
- そうした残念な対策の光と影について説明します

メール添付ファイルの暗号化

Light

- 個人情報保護法から大騒ぎ
- 電子メールはハガキと同じ、経路途中での盗聴リスクあり
- 暗号化すれば盗聴されることはない
- 送信時にサーバ側で自動で暗号化して、パスワードを別メールで自動送信すれば漏れなく暗号化できる
- 添付ファイルの拡張子exeを受信時にフィルタしているケースに対しても、ex_やex_eに拡張子を変更することで、完璧な対応

メール添付ファイルの暗号化

Shadow

- 同じメールサーバから同じ経路でパスワードを送信したら、盗聴対策にならない
- 経路途中での盗聴による情報漏えいの事例はNSA以外には聞いたことがない
- むしろ暗号化したために、ウィルスが検出できずにクライアントに直接届くケースが発生
- 最も簡単にexeファイルを実行させることができる
- 標的型攻撃と親和性が高い

ログ統合監視による内部不正検知
Light

- 内部統制の要求事項の難題
- 管理者権限は何でもできる
- 管理者権限で決算情報を改ざんされたら、深刻なリスクだ
- 管理者権限を使う運用を疑え！
- 操作ログを収集・保管し、証拠保全して牽制しよう
- Windows画面上のマウス操作に対しては、画面操作を録画して動画で証跡を保存

ログ統合監視による内部不正検知

Shadow

- 決算に対する深刻な不正は経営陣が行うので牽制効果なし
- 運用のオペレータが不正に関わった深刻事例なし
- 実行権限はあるが何をしているか、中身を知らないのが運用
- 対策費を捻出する経営側やスキームを提案するコンサル側が、むしろ内部不正を行ったり、看過してしまう側
- 相手を間違えた監視
- 仕事を増やすだけ

データセンターでの手荷物検査
Light

- データセンターの安全・信頼性に係る情報開示指針（総務省）
- メディア、USBメモリ、携帯電話の持ち込みを禁止
- カメラ付き携帯電話は撮影により情報漏えいするから厳禁！（ビジネス用途でカメラ無しガラケーもあったよね）
- 持ち込み申請書、抜き打ち検査、ロッカー設置、持込みには透明なビニール製バッグを使わせる等で徹底
- ポケットのない制服をオペレータに着せているデータセンターもあるよ

データセンターでの手荷物検査

Shadow

- 不正に持ち込みたい奴は服とか下着、靴下とかに簡単に隠して持ち込める
- ルールを順守しようとする人に負担になるだけ
- 牽制の意味で、そこそこ実施するのはよいが、過信、過剰徹底は無意味
- 正義（正しい運用）を挫き、不誠実な者を見逃す逆効果な対策

最新のインテリジェンスビル
Light

- ISMS認証基準、PCI DSS「データ環境へのアクセス管理」
- セキュリティゲート、認証ドア、エレベータでもICカード認証で停止階を制御
- 非常階段側にも認証ドアで、宅配業者の入館も制御
- 飲食スペースも充実して外出を少なくする、仕事納めや新年会をビル内で行うことで、酔いすぎて鞄を紛失するなどの飲酒トラブルを防ぐ

最新のインテリジェンスビル

Shadow

- 壁面がガラス張りの場合、向かいのビルから画面やホワイトボードが見える
- 紳士の社交場・喫煙コーナーが無いことが増えている
- 社外の喫煙スペースで吸う
- 取引先への電話など、簡易な事務に喫煙スペースは最適
- 会話から機密情報が漏えい
- 上場企業の本社が集まる丸の内の某所、寒空の中で

Smoking！　Smoking！

IDカードによる入退室管理

Light

- ISMS認証基準「物理的入退管理策」
- セキュリティゲートや認証ドアにより、第三者の侵入を防ぐ
- セキュリティゲートは連れ入り（ピギーバック）も防止し、データセンターを強固に守る

IDカードによる入退室管理

Shadow

- 高層ビルは多くの会社が入居しており、自社用にセキュリティゲートは設置しづらく、認証ドアでの対策が中心となる
- 認証ドアでは、連れ入りが可能
- 認証をICカードから指紋に変えても同様に連れ入りが可能
- 始業時、昼休みの開始、終了時、派遣職員の定時退社など、ドアが頻繁に開く時間帯は簡単に入れる
- トイレはほとんどの場合、認証ドアの外側にある
- トイレで歯磨きしながら、誰かがトイレに来るのを待ち伏せ可能

IDカードによる入退室管理
＋ Shadow

- 大手町のランチに行ってみよう
- 銀行のロゴ入りのストラップを首から下げたまま、本社の幹部社員が昼飯を食っている
- 会話から機密情報が漏れる可能性あり
- 不祥事、統廃合の時はマスコミが関係者のコメントを拾おうと張り込んでいる
- 社外に出るときはストラップを外せ、とまで言っている会社は聞いたことがない
- ストラップを外すよう言えば、IDカードをなくす奴が発生する
- 名前と所属を首から晒しての外出はソーシャルのターゲット

まとめ

ダメなセキュリティ対策の特徴

- 盗聴など情報漏えいには、とにかく暗号で対策
- ICカードや指紋は、偽造できないからセキュアだと妄信（運用は考えない）
- 上から目線で、業務の現場を縛る、禁止する、監視する（経営層＝自分だけを聖域にする）
- 最新鋭や高価な対策は、効果が高いと考える（判断基準に、効果ではなく費用の大小を用いる）
- 「横並びでやっとけ」という効果を考えないで導入する対策

その結果、高価な対策が台無しに！

無駄な対策はしない！

対策するなら費用分の効果を出そう！

ご清聴ありがとうございました

e-mail　　：aido@hkg.odn.ne.jp
Facebook　：Hiroshi.Aido　相戸 浩志