JANOG34 Meeting in TAKAMATSU 2014.07.18

みんなで高める セキュリティ

Internet Initiative Japan Inc.
Yasunari Momoi
<momo@iij.ad.jp>

自己紹介

- ももいやすなり
  - Twitter **@sbg**
  - Facebook **ymomoi**
- 開発、セキュリティ、勉強会
  - 食べ物、ロック/メタル、ねこ
- IIJ 本社移転: 神保町から飯田橋へ
- IIR
  - http://bit.ly/IIJ-IIR
  - http://bit.ly/IIJ-IIR-EN (英語版)
- IIJ Security Diary (マニア向け?)
  - https://sect.iij.ad.jp/

昨今のセキュリティ事件

- 色々な種類のものがありますが…
- 組織的、大規模化、巧妙化
  - ツール・脆弱性市場、キャンペーン
- 標的型攻撃
- フィッシング、水飲み場攻撃
  - オンラインバンキングが狙われる（実利がある）
- 複合的な手段をとることも多い

ユーザとパスワード

よく使われるパスワード 2013年版

Password

先週 SpalshData が "Worst Passwords of 2013" のリストを発表しました。SpalshDataはパスワード管理ソフトなどスマートフォン向けの製品を開発している会社ですが、その年に起きた情報漏洩事件のデータをもとに、ユーザがよく使うパスワードのトップ25を調べて、2011年から毎年発表しています。

- 2013年 "Password" unseated by "123456" on SplashData's annual "Worst Passwords" list
- 2012年 Scary Logins: Worst Passwords of 2012 — and How to Fix Them
- 2011年 When "Most Popular" Isn't A Good Thing: Worst Passwords of the Year – And How to Fix Them

リストの変遷を表にしてみました。

順位	2011年	2012年	2013年
1	password	password	123456
2	123456	123456	password
3	12345678	12345678	1234567
4	qwerty	abc123	qwerty
5	abc123	qwerty	abc123

順位	全体での順位	暗号化されたパスワード (Base64)	パスワード (推測)	該当者数	%	パスワードヒントの例
1	1	EQ7fIpT7i/Q=	123456	4652	0.54	654321, 1〜6, number
2	2	j9p+HwtWWT86aMjgZFLzYg==	123456789	1265	0.15	suuji, 987654321
3	5	j9p+HwtWWT/ioxG6CatHBw==	12345678	890	0.10	1-8, 1〜8, 87654321
4	3	L8qbAD3jl3jioxG6CatHBw==	password	819	0.10	pass, simple is best, pasuwa-do, P@ssw0rd
5	8	7LqYzKVeq8I=	111111	720	0.08	1*6, simple number, 222222

- 古典的だが今でも効果的
  - ユーザ ID の共通化？
  - 更新されないシステム
- パスワードリスト攻撃
  - 大規模流出事件
- 脆弱なパスワード利用
  - 管理画面のデフォルト

引用:
セキュリティは楽しいかね？
2014-01 記事

必要なこと

- 組織が生き残るために
  - 情報共有
  - 連携しての事案対応
    - 実際には難しいケースも
- みんなが困らないために
  - 当たり前の防御
    - ウイルス対策ソフト
  - 利用者のリテラシ向上
    - IoT
- リテラシが高い人は…

今、我々ができることは？

今、我々ができることは？

伝えること

“セキュリティ関係者は知恵の拡散に従事せよ”

–Jeff Moss (Black Hat 創設者)

引用: エンジニア type: 2014/02/19
「セキュリティ関係者は知恵の拡散に従事せよ」Black Hat創設者Jeff Moss氏からの提言
http://engineer.typemag.jp/article/codeblue_jeffmoss

“目指すは『an・an』でセキュリティ男子特集が組まれること！”

–辻伸弘 (ソフトバンク・テクノロジー)

引用: エンタープライズジン Securityプロに会いたい！ 2014-04-22
イケてるセキュリティ男子に、俺はなる！―ソフトバンク・テクノロジー　辻伸弘さん
http://enterprisezine.jp/iti/detail/5777

周囲の「普通の人」に伝える

- 自衛手段を伝える
- パスワードの例:
  - パスワードを使い回さない
  - パスワードの管理方法
    - 紙に書く、俺ルールを作る
      - 物理セキュリティに頼る
    - パスワード管理ソフト
- すぐにできることを
  - 状況を今よりも少しよくする！

社内でもの申す

- 例: 新しいサービスをローンチ
  - そもそも認証が必要か？
  - よそを頼れないか？
    - よらば大樹の陰 (OpenID とか)
  - 十分な対策をしたか？
    - 監視、二要素認証、…
  - 更新を続ける覚悟はあるか？
  - 必要ない情報を集めてないか？
- 自社のサバイバビリティを上げる！