SEAGULL 通信

令和元年10月21日発行

No. 8

"security action for guarding technical intelligence"

ソーシャルエンジニアリングをご存知ですか・・・

ソーシャルエンジニアリングとは

人の心理的な隙やミスにつけ込み、ネットワークにログインするためのパスワード等の重要情報を、IT技術を使用しないで盗み出す手法のことをいいます。

つまり、物理的な情報セキュリティ対策を講じたとしても、注意不足によって、悪意のある人物により情報が盗まれることがあるのです。
本号では、ソーシャルエンジニアリングの一例を紹介したいと思います。

その１～ショルダーハッキング～

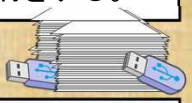
人がパスワードなどの重要な情報を入力している時に後ろから近づいて覗き見ることです。

対策
- ○ 重要な情報をタイピングする時には、周囲に人がいないことを確かめる。
- ○ ディスプレイにフィルタを貼る等して、覗きにくいようにする。

その２～トラッシング～

アクセスしようと狙ったネットワークに侵入するために、ゴミ箱に捨てられた紙媒体や記憶媒体等から、ネットワークに関する内容やユーザー名やパスワード等の情報を探し出すことです。

対策
- ○ 確実にシュレッダで裁断する。
- ○ 磁気データの廃棄の際は、消磁や物理的破壊などで確実なデータ抹消をする。



その３～電話を利用したパスワードの聞き出し～

何らかの方法でユーザ名を入手して、その利用者になりすましてネットワークの管理者に電話をかけて、パスワードを聞き出したり、パスワードの変更を依頼する。また、管理者になりすまして、利用者からパスワードを聞き出す手法を言います。

対策
- ○ パスワードの問い合わせなどに対する処理設定、手順、本人確認方法を整備する。
- ○ 電話ではパスワードなどの重要情報を伝えない等のルールを設定する。

あなたの会社の大切な情報を隙のない管理で護りましょう!!

しーがる川柳

利用価値　知らずに捨てる　狭い視野

しーがる川柳公募中!!
SEAGULL通信で紹介させていただきます。

▼ SEAGULL事務局（外事課内） ▼

〒231-8403　横浜市中区海岸通2丁目4番　神奈川県警察本部

相談窓口　Email：seagull@police.pref.kanagawa.jp