サイバーセキュリティタスクフォース

資料２－２

IoTセキュリティ対策について

株式会社FFRI
鵜飼裕司

概要

- 論点

  - 考察すべき対象は家庭用ルーターから産業用機器まで幅広く存在
    → 対象の整理・検討

  - 現状と将来のIoT機器、システムに対する課題と対策の整理
    → 時間軸における整理・検討

  - 対策、啓発活動など費用負担者および実施者の検討
    → メーカー、ユーザー、ISP事業者、国、など、負担者・対策実施者の整理・検討

- 前提

  - 「脅威」をどう捉えるか? – 誰にとって、どのような脅威を想定して対策するのか
  - 対策は困難 – 部分的な情報や想定される脅威があるだけで、現状把握が出来ていない

  現状、非常に大きな脅威がある可能性もあれば限定的である可能性も。
  現状や新しい仕組みの脅威分析があまりなされていないため、将来的な脅威も予測しにくい

対象の整理・検討

- 考察すべき対象は家庭用ルーターから産業用機器まで幅広く存在
- 産業用機器等、一部は重大なインパクトを与える可能性もあるが、家庭用ルーター等も大量にハッキングされれば重大なインパクトに成り得る可能性も
- ただし、適切な対策のプロセスは大きく異なる事が想定される
  -技術的に対策する事は可能だが・・・
  - 家庭用ルーターと高価な産業用機器ではビジネスモデルが大きく異なる
  - ユーザーのリテラシー、周知方法、コスト負担に対する考え方などが大きく異なる
- そもそも、どのようなものを対象とすべきかを決める上でも、より深い現状把握を実施する必要がある

現状と将来のIoT機器、システムに対する課題と対策の整理

- 現状のものは、運用、あるいはシステムの持つセキュリティ上の課題を解決する必要がある
  - パスワードの変更、運用方法の見直し、脆弱性の修正、etc

- 将来的なものは、より安全に運用できる仕組みや、機器の安全性を上げるための仕組みを開発のプロセスに入れる必要がある
  - パスワードの強制設定、アップデート、セキュアな設定、セキュアデザイン・コーディング等

- ただ、それぞれの機器、システムにおけるビジネスモデルに強く依存する
  - セキュリティが市場において競争優位性とならない場合は、メーカーに強い動機は発生しない

対策、啓発活動など費用負担者および実施者の検討

- 誰が、どのような対策を実施し、どのように啓発するのか
- 誰が費用負担するのか
- 明確なインセンティブ(競争優位性の確保など)が無ければ、事業者が自力で対策を推進する事は困難
- ユーザーが運用でカバーできる対策も、適切な啓発活動が行われ、ユーザーにとって明確なインセンティブが無ければ対策は進まない可能性
- 国が一定の推進力にならないと進まないのでは？

対策の進め方

- 国がイニシアチブを取って進める必要があるのではないか？
- そのためには、
  - 適切な現状把握
  - 現状把握により得られた事実と、将来的なICT関連技術の分析により、適切な脅威分析を実施する必要がある
- 正確な脅威分析が行われれば、想定される脅威について妥当性のある対策が推進できる
- 現状把握をできる仕組みの構築が重要

現状把握の概要

- 「SHODAN」のような仕組みを実現できないか？

  - 日本のIPアドレスをクロールし、どこに何が接続されており、どのような問題があるのか把握する広域脆弱性スキャンの実施

  - 脆弱性については、対象機器の特定技術(Banner Scan、OS Fingerprinting、Protocol Analysis等)と脆弱性データベースを充実させる事で、非破壊かつ不正アクセス禁止法に触れない形である程度洗い出せる

広域脆弱性スキャンの課題

- ブルートフォース等による認証突破については検討すべき課題がある。
  しかし、攻撃側は実施しているため、より正確な現状把握のためにも例外措置など検討できないか
- 商用のスキャナを活用できる可能性があるが、国内のIPアドレスを総当たりするとなると費用が高騰する可能性があり、かつ、細かいチューニングやタイムリーな追加開発ができない
- 利用できる組織をどのように限定するのか
- ネットワークに対する負荷
- 脆弱性スキャンやブルートフォースにより、対象の組織に不要なインシデント対応を強いる可能性
- スキャナの開発や運用は、技術的には枯れておりハードルは小さい。技術以外の壁が大きいのではないか