第 16 回電力 SWG
参考資料 2

産業サイバーセキュリティ研究会電力 SWG における意見

2024 年 2 月 1 日

一般社団法人 JPCERT コーディネーションセンター
政策担当部長　兼　早期警戒グループマネージャ
脅威アナリスト
佐々木　勇人

大変恐縮ながら、第 16 回会合には都合により欠席となるため、事務局からの資料及び事前説明に対するコメントとして以下の通り記します。今後の検討の参考になれば幸いです。

〇リスク管理全体のアプローチについて

従前は、コンプライアンス型アプローチが取られてきており、各種ガイドライン、フレームワーク、基準、指針等と自組織の現状とのギャップを明らかにし、改善を図っていくことが取り組まれてきました。しかしながら、最近では IT サプライチェーンの問題や委託先管理、クラウド上のデータ管理など、責任分界点の整理と管理が難しい状況が増え続けており、コンプライアンス型アプローチの限界も見えてきています。

そうした中で、脅威ベースアプローチに基づき、アクターや悪用される蓋然性のある脆弱性などの情報を積極的に入手・補完し、対応の優先順位や脆弱な箇所のピンポイントでの速やかな対処などの取り組みが各所で進みつつあります。ISAC をはじめとした情報共有活動もこうした脅威情報の入手経路として活用が進んでいるかと思いますが、業界全体としても、また、新規参入事業者も含めて、脅威情報の入手、情報共有の活用の観点がより重要になってくると考えています。

〇サプライチェーンリスク対応について

国内において「サプライチェーン攻撃」といった場合子会社やグループ企業をはじめ、「被害組織よりも対策の弱い関連先経由で侵害するケース」が取り上げられがちなところ、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」等でも示されている通り、基本的には、ソフトウェアや IT サービスの供給経路に係るリスク管理がメインのテーマであり、事務局提示資料のほか、国内外で事案として顕在化したものとしても後者が大半です。

弊センターで懸念している点としては、

① ソフトウェアの脆弱性が悪用された攻撃が発生した場合、脆弱性情報自体は公表・流通していても、「当該脆弱性の悪用事実」については伝達されないケースが多く、被害拡大につながっている

② いわゆる運用保守ベンダ自身が攻撃の“踏み台”となってしまい、提供するサービス／製品の供給経路が侵害されてユーザー組織側に被害が出る事案が度々発生しており、影響をうける対象者への速やかな情報提供がなされなかったり、事案の詳細解明において外部の専門知見が活用されにくいケースが多く、原因究明、再発防止策が不徹底に終わっている

③ VPN 経由等で遠隔保守を行っている、いわゆる運用保守ベンダが利用／提供する機器／経路から侵害されるケースがあるところ、ファーストレスポンダーとして調査にあたる者も当該ベンダであるため、原因特定が不透明なままクローズしてしまうケースがあり、原因究明、再発防止策が不徹底に終わっている

の大きくは3点あります。①については、ベンダ側が悪用事実について開示を避けるケースと、商流上、悪用事実に関する情報が伝わらないケースがあり、それぞれ弊センター等からも問題提起している次第です。

②、③ついては、使っている製品、システム構成、契約形態など多種多様であるため、前述の通り、チェックリストなどの従前からのコンプライアンス型アプローチでの対処は困難です。また、この問題への対策もユーザーサイドでできる範囲は限られており、ベンダ側における脅威情報提供の役割の明確化というセキュリティ政策全体の課題である点も同様です。

当該問題については本 SWG の検討スコープというより、より広いセキュリティ政策全体の課題であるところ（※詳細は後述の「参考情報」をご参照ください）、実際に影響を受けるユーザーサイド／各産業分野側として本 SWG でも取り上げるべき課題と考えます。

＜参考情報＞

・ベンダから製品・サービスの悪用に関する情報が開示／提供されにくい問題について
経済産業省　産業サイバーセキュリティ研究会「サイバー攻撃による被害に関する情報共有の促進に向けた検討会 報告書等」

頁「サプライチェーンにおけるベンダ等の役割について」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/pdf/20231122_2.pdf

同検討会「攻撃技術情報の取扱い・活用手引き（案）」64 頁「脆弱性悪用に関する情報はどうハンドリングされるべきか」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/pdf/20231122_3.pdf

・商流上、脆弱性情報や悪用に関する情報が流通していない問題について
JPCERT/CC「なぜ、SSL-VPN 製品の脆弱性は放置されるのか ～“サプライチェーン”攻撃という言葉の陰で見過ごされている攻撃原因について～」
https://blogs.jpcert.or.jp/ja/2022/07/ssl-vpn.html

〇ERAB、その他新規参入事業者全体のセキュリティ対策向上について

こちらも、ガイドライン、チェックリスト、チェックツールといった一般的なリスク管理のアプローチでは限界があるところ（※なんらそれらの取り組みを否定するものではありません)、ここまでに記した通り、脅威情報の入手が課題であります。

特に、ERAB など、新エネルギーの活用システムにおいては、いわゆる IoT 機器の活用に伴い、インターネットから到達可能なデバイスの増加が必然であり、こうした製品の脆弱性情報の流通に課題があると考えています。

直近では、SolarView Compact の脆弱性（CVE-2022-29303）の悪用についてメディアで取り上げられたり、海外当局からのアラート情報に掲載されるケースがありましたが、従前の脆弱性情報流通でもまだ取り扱い件数が少ないこうした分野の機器の脆弱性情報については、製品やサポート情報の供給メカニズムが一般的なソフトウェア製品と異なる点もあり、メーカーからユーザーまで情報が到達しにくいケースも散見されます。

この分野においても、冒頭に述べた通り、コンプライアンス型のアプローチに加えて、(脅威）情報という観点に着目した脅威ベース型のアプローチの観点も今後必要であると考えます。

以上