Optimizing Your Security

iSiD

IPAの10大脅威に急浮上、「サプライチェーン攻撃」対策に現実解はあるか

従来までセキュリティというと、自社の対策のみで済んでいたかもしれない。しかし近年では、IoTの普及もあり、部品の調達から、製造、在庫管理、物流、販売、業務委託までを含めた一連の商流のなかで、セキュリティを見なければいけない時代になった。対策の甘い関連企業から攻撃を仕掛けられ、そこを踏み台に本社まで狙われるリスクがあるからだ。このような時代に企業セキュリティを盤石にする術はあるのか。


情報セキュリティ10大脅威 2019 脅威ランキング IPA

「個人」向け脅威	順位	「組織」向け脅威
クレジットカード情報の不正利用	1	標的型攻撃による被害
フィッシングによる個人情報等の詐取	2	ビジネスメール詐欺による被害
不正アプリによるスマートフォン利用者への被害	3	ランサムウェアによる被害
メール等を使った脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した攻撃の高まり
ネット上の誹謗・中傷・デマ	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	サービス妨害攻撃によるサービスの停止
インターネットバンキングの不正利用	7	インターネットサービスからの個人情報の窃取
インターネットサービスへの不正ログイン	8	IoT機器の脆弱性の顕在化
ランサムウェアによる被害	9	脆弱性対策情報の公開に伴う悪用増加
IoT機器の不適切な管理	10	不注意による情報漏えい

Copyright © 2019 独立行政法人情報処理推進機構 4

IPAが発行する「情報セキュリティ10第脅威」のレポートで、今年の新たな脅威として、第4位に「サプライチェーン（商流）の弱点を悪用した攻撃」が初登場した。（出典：独立行政法人情報処理推進機構発表を一部加工）

IPA調査でいきなり「第4位」に浮上した新たな脅威

IPA（独立行政法人情報処理推進機構）が毎年発表している「情報セキュリティ10大脅威」のレポートで、今年初めて第4位に登場した組織向けの脅威がある。それは「サプライチェーン（商流）の弱点を悪用した攻撃」だ。

従来は自社のセキュリティ対策で済むことも多かったが、いまはグループ企業や海外法人、関連取引先まで含め、全体の対策を実施しなければならない。攻撃者はセキュリティの甘い組織の穴を見つけ、そこを攻撃の足掛かりに狙ってくるためだ。

実際、昨年起きた事例では、ある製造系企業の委託企業が標的型攻撃を受け、そこから関連会社のメールアドレス情報が漏れてしまうというインシデントの報告もあった。製造業も最近はIoTで接続先も増え、脅威の範囲も広がっている。

そのためIPAでも、外部の委託企業などから自社に被害が拡大しないように、適切な情報セキュリティ管理を喚起しているものの、まだ製造や卸売・小売業では、実施すべきセキュリティ対策をしっかりと明示しない企業が7割にも上るという。

そこで企業側は、関連会社はもちろん委託企業に対しても、業務の範囲・セキュリティの要件・罰則の規定などを契約に明記することで縛りをかける、あるいはシステムの脆弱（ぜいじゃく）性診断サービスを定期的に実施してもらうことでセキュリティ対策を進めている。

とはいえ、たとえ契約で縛っても、それはあくまで机上の話だ。現実問題としてどんなリスクが企業に潜んでいるか分からない。また脆弱性診断を行うのも、そう簡単なことではなく、相応のコストもかかる。診断時には疑似攻撃をかけるので、システムに負荷がかかり、計画から実施までIT担当者の大きな負担になってしまう。

攻撃者の目線からセキュリティ状況を把握、簡単かつ迅速にスコアリング

こういった課題を解決するために注目を集め始めたのが、攻撃者の目線で企業のセキュリティ対策状況をスコアリングすることができるスコアリングサービスだ。

標的型攻撃を行う攻撃者の手口を見ると、偵察→配送→攻撃→インストール→遠隔操作→侵入拡大→目的達成というように、特定のターゲットに対して、サイバー攻撃を仕掛けてくることが一般的な流れだろう。これらの負の連鎖をどこかで断ち切るためには、「攻撃者の目線」からセキュリティ状況を把握することが求められる。

加えて、自社につながるサプライチェーンにおいて、それぞれのセキュリティ対策の状況を可視化し、見つかったセキュリティ上の課題に対して改善していくことが求められる。

そこで威力を発揮するのが、電通国際情報サービスが提供する米・SecurityScorecard社（以下、SSC社）のセキュリティ・スコアリング・サービス「SecurityScorecard」だ。

本サービスは、インターネット上から収集された情報をベースに、攻撃者の視点でセキュリティ上どのような問題があるか、可視化し詳細に分析できるサービスだ。

ハニーポットやダークウェブも含めたインターネット上から独自に情報を収集。その情報をもとに企業のセキュリティリスクをスコアリングする。電通国際情報サービスの赤澤 卓真氏はこう話す。

「これまでに全世界800顧客の大手企業で実績を積み、スコア化を行った企業数は100万社以上。と多くの経験と実績を持つサービスです。日本では2019年6月5日に弊社から提供し、現在すでに多くのお客様にPoCを実施いただき、その中から既に導入頂き実際に運用頂いているお客様もいらっしゃいます。対象システムに影響を与えないことから、比較的容易にPoCを実施いただき、実際の運用イメージが掴みやすい事から、スムーズに導入頂いております。」（赤澤氏）

SecurityScorecardの最大の特徴は、「利用方法がとても簡単」であることだ。調査対象のドメインを入力する。それだけで自社のリスクを数値として点数化し、現時点のセキュリティ状況を瞬時に表示してくれる。

「従来の脆弱性診断のようにシステムに負荷をかけることなく、素早くセキュリティの甘い部分を調べられます。もちろん自社のみならず、これまでチェックが難しかった関連会社や委託先などのサプライチェーンも含めて、簡単に調査することが可能です」（赤澤氏）

後ほど詳しく説明するが、現状のセキュリティの点数がはじき出されたら、対策が不十分なステークホルダーに対して“合格ライン”を設定した上で指示することもできる。


電通国際情報サービス
金融ソリューション事業部
営業企画部
赤澤 卓真 氏

SecurityScorecard社
VP
Matthew 氏

SecurityScorecard

SecurityScorecardのスコアリングの流れ。調査対象のドメインを入力するだけで、SSC社がデータ収集して得た情報をベースにリスクを数値として瞬時に点数化する。

目標レベルを設定し、具体的な推奨のセキュリティ対策まで示唆

ここからは、SecurityScorecardの機能について、もう少し詳しく説明しよう。この本サービスを受けると、サマリーレポートのほかに、各種の詳細レポートを作成できる。

サマリーでは、全体スコアとともに、「Application Security」「Network Security」「Endpoint Security」「Patcing Cadence」「Hacker Chatter」など10個（計77個）の分類ごとに、各点数とA～Fまでの5段階の指標を表示。発見された脆弱性の件数や分類も示される。

SecurityScorecardのサマリーレポート。全体のスコアとレベル、発見された脆弱性の件数や分類も表示。また業界標準と比べ、どのくらいの位置にいるのかも把握できる。
※本レポートは英語表記となっているが、日本語など言語切り替えも可能。

「たとえば『外部からサーバの不要なサービスにアクセスできないか』『DNSのセキュリティは正しく設定されているか』『公開しているサーバで緊急度が高いパッチは速やかに適用できているか』『社員が脆弱なブラウザを使ってインターネットにアクセスしていないか』といった事項に加え、インテリジェンスを駆使してハッカーの動向を監視し、攻撃の標的にされていないか調べるなど、さまざまな角度から問題を洗い出してくれます」（赤澤氏）

もし分類の中で点数の低い項目が発見されたら、さらに細かい項目を調べることで問題点をあぶりだせる。対策を打った後で、点数がいくら上がるかもシミュレーションして表示。

レポートは相手側と共有でき、現状の指標がCレベルならば、目標としてBレベルに設定し、推奨される具体的なセキュリティ対策を示すこともできる。

また、スコアリングの推移は過去にさかのぼって見られるため、どのようにセキュリティが改善されたのか、その経緯を追うことも可能だ。ユニークな点は、自社を含めた調査対象が所属する業界で、同規模の企業平均スコアをレーダーチャート上で比較できること。これらのレポートによって、他社との比較が一目瞭然になるため、経営者に見せれば、セキュリティの実情を十分に理解してもらえるだろう。

問題点を詳細に表示して把握することが可能。さらに具体的にどの改善タスクを実行すれば、スコアがアップするのかもシミュレーションできる

現状の指標から目標となる指標を設定し、その指標に必要なスコアにするために求められる改善策を、入手した推奨プランなどから検討できる

政府御用達の製造業のほか金融業界での活用も

SecurityScorecardを活用すれば、企業やグループ内でのセキュリティ診断のセルフチェックだけでなく、取引先に求めるセキュリティレベルを提示してリスクマネジメントも実施できる。このほかにも、もともと金融業界に強みを持つ電通国際情報サービスでは、保険会社のサイバー保険や金融機関の企業の査定・調査への活用など、幅広い用途でのサポートを検討している。

すでに海外では、金融系では米CadenceBankが上位40社の重要な取引ベンダーのDD（Due Diligence）を行う際にSecurityScorecardを使って、サイバーセキュリティの観点からリスクを迅速に判断しているという。レポートが見やすく、判断基準が明確で、セキュリティの専門知識がなくても使えるので重宝しているそうだ。

またSecurityScorecardは、米国政府の調達品を製造する企業などで新セキュリティ標準となる「NIST SP800-171」への対応にも役立つ。「NIST SP800-171」は、米国防省と取引がある全世界の企業を対象とするガイドラインだ。2019年度以降、日本でも防衛省と取引がある企業に適用されることになったため、政府調達のサプライチェーンでつながる企業も含めて影響を及ぼす。SecurityScorecardを使えばこの「NIST SP800-171」をはじめ、さまざまなガイドラインごとに照らし合わせた診断結果を即座にチェックできる。グローバル化が進む今後、ますます本サービスは有用になるだろう。

「我々は、"Optimizing Your Security"というスローガンのもとに、多くの企業のお手伝いをしてきました。このサービスをご利用いただき、もし何か問題点が判明したら、具体的で現実的な対策をお客さまと一緒に考えながら、最適な環境づくりをご支援していきます。我々がこれまで培った"SIer力"を信頼してください」（赤澤氏）

このSecurityScorecardを導入することで、自社や関連企業を含めたサプライチェーン全体から脅威を排除し、より盤石なセキュリティ体制を構築することができるようになる。IPAが警戒するサプライチェーン攻撃への新たな対策手段として、ぜひ検討してはいかがだろうか。

ソリューション紹介サイトはこちら

SecurityScorecard

AIやIoTの進展に伴い、サイバー攻撃による経済的・社会的損失の発生リスクは拡大の一途を辿っています。中でも、セキュリティ対策が脆弱な取引先や子会社等を経由して大企業に攻撃を仕掛ける「サプライチェーン攻撃」の被害は年々深刻化しています。
SecurityScorecardは、そのようなサプライチェーン攻撃へのリスクを瞬時に点数化し、改善すべきポイントを可視化するスコアリングサービスです。自社だけでなく、サプライチェーン全体のセキュリティ対策状況を把握することができます。

iSiD 株式会社電通国際情報サービス（略称 ISID）
金融ソリューション事業部　営業企画部
〒108-0075 東京都港区港南 2-17-1
E-mail：g-security@group.isid.co.jp
Tel：03-6713-7030