被害後のダメージコントロールの切り札、3つの分類で理解するCSIRT構築の方法

現在、人の過失、あるいは人をうまく騙して脆弱性を突くサイバー攻撃が顕著になってきている。しかし、人が狙われると、それを100%防ぎ切ることは難しい。そこで重要になるのが、自社システムに侵入されることを前提とした“ダメージコントロール”だ。迅速かつ適切な初動対応によって被害の拡大を抑え、さらに被害の出ている状況を短期間で終息させるための体制作り、即ちCSIRT(Computer Security Incident Response Team)の構築が重要だ。

デロイト トーマツ リスクサービス
マネジャー
森島 直人 氏

人をリスクとして認識し、被害後のダメージコントロールを考える

今、サイバー攻撃のターゲットとなっているのが「人」だ。たとえば攻撃者が業績情報を盗りたい時には経理担当者が、特許／知財関連の情報を盗りたい時には研究者が、また親企業への攻撃が難しい場合には、関連する子会社や取引先の担当者が狙われることになる。

デロイトトーマツ サイバーセキュリティ先端研究所主催の第2回サイバーセキュリティセミナー「CSIRTと情報開示～攻めのレピュテーションコントロール～」で登壇した森島氏はその理由について、「現在のサイバー攻撃が非常にビジネス化しているから」と指摘する。

「攻撃者はいかに“高価な”情報を奪い盗るかと同時に、いかに“安価に”攻撃を成功させるかを考えています。一方で、情報セキュリティ関連のテクノロジーは非常に進歩しており、対策をきちんと施している企業に対しては攻撃者も正面突破は簡単ではありません。そこで弱いところ、つまり“人”がターゲットにされます。これは、人を狙う方法が安くつくからなのです」。

そしていったん高価な情報を発見すると、攻撃者は執拗にその企業を攻撃する。特に相手が人の場合、何回か攻撃を繰り返すと成功することもある。そこで現在、標的型攻撃が増えているという。

「人をターゲットにされた場合、執念深く繰り返される攻撃を100%防ぎ切ることは非常に難しいでしょう。そこで重要となるのが、いったん被害が出た後、その被害をいかに最小限にするかという取り組みです。これを“ダメージコントロール”といいますが、現在ではこの取り組みが企業に求められています」。

侵入の早期発見はSOCやMSSで、発見後の対応はCSIRTで

ではその取り組みは、どのように進めていけばいいのだろうか。まず早期発見のための基本的な対策としては、エンドユーザーの利用する各種デバイスやネットワーク機器のログのモニタリングが非常に重要となる。ただしそれだけでは不十分で、次に個人端末やメールサーバ、あるいはプロキシサーバなどの各ログをうまく紐付けて相関分析を行い、怪しい動きをしている特定の連続したイベントが発生していないかもチェックする。それがSIEM(Security Information and Event Management)と呼ばれる取り組みだ。

「セキュリティ監視を行うSOC(Security Operation Center)を構築し、あるいは社外のMSS(Managed Security Service)を活用し、SIEMも採り入れて発見の仕組みを作っていくことが求められます」。

次に侵入発見後は、被害拡大を一刻も早く終息させるための取り組みが重要だ。

「それがインシデント対応専任チームであるCSIRT(Computer Security Incident Response Team)の構築です。SOCもしくはMSSとCSIRTの組み合わせで、うまくダメージコントロールしていくことが肝要です」。

CSIRTは「仮想型」「単一型」「コーディネーション型」の3タイプに分類

続いて森島氏は、CSIRTの活動内容と組織形態について、詳しい説明を行った。まず日常的活動としては、体制の整備や社内情報の収集、関連するシステムの運用維持、情報収集、インシデントデータベースの構築、リスク分析、従業員の教育などが挙げられる。また事後活動としては、証跡の分析と原因究明、適切なマネジメント層への報告、インシデントデータベースの更新、対応手順の検証と見直しなどが挙げられる。

そしてCSIRTの中心的な活動となるインシデント対応では、インシデントの検出後、[トリアージ→意思決定と対処]を繰り返すことで、同時多発的なインシデントに対応していく。

また、CSIRTは、「仮想型」「単一型」「コーディネーション型」という3タイプに分類できる。その際、情報アクセスのレベルやサービス停止の可否、その他意思決定の権限をどこまで持たせるかによって、さらに色々な選択肢が考えられるという。

まず仮想型CSIRTでは、チームを構成するメンバーはユーザー部門と兼務で、有事の際に集まって対処し、対応が終われば解散する。短時間でCSIRTを立ち上げられるというメリットがある一方、予算の確保や人事評価が困難、日常的活動が手薄になるなどの課題がある。

次に予算があり、頑健な対応が必要な場合の選択肢としては、単一型CSIRTがある。独立した組織運営を行うタイプのCSIRTで、日常的活動が可能となり、組織上の位置付けも明確になるが、多様な人材を確保する必要があり、構築に時間がかかるといった課題がある。

そして3つめがコーディネート型CSIRTで、各ユーザー部門に小さなIRT(Incident Response Team)を設置し、各々を取りまとめるコーディネーションセンタ(CC)を設置する。CCはコーディネートのみに専念し、実際の対応は各IRTが行う。CCは常設機関なので日常的活動もしやすく、子会社も含めて統括することが可能になるが、各IRTの対応品質がバラついたり、IRT間の連携遅延が発生する可能性もある。

「考えるべき大切なポイントは2つあります。1つめは、自社システムに侵入されてから、それを発見するまでの時間をいかに短くするか、そして2つめは、対応を開始してから終息させるまでの時間をいかに短くするかです。早く発見できれば対応も早く開始でき、その分、終息までの時間も短縮できます。この2点が損害額を最小限に抑えるための鍵であり、そのためのCSIRTなのです」。

なぜあの企業は叩かれるのか?
ピンチをチャンスに変える「攻めの情報開示」

ひとたびインシデントが発生した時、可及的速やかにその脅威を排除することは必須の対応だ。加えて社会的責任を負う企業や組織では、そのインシデントに関する情報を関係各者に開示していくことも求められる。しかしその情報開示が適切に行われなかった場合、憶測や風評の流布によって二次的な損失が発生する恐れが十分にある。デロイト トーマツ リスクサービス シニアマネジャーの亀井将博氏は、「ソーシャルメディアが情報拡散の主力媒体となった今日、レピュテーション(=評判)によるリスクは事業継続を脅かすまでになっています」と指摘、「一方で適切な対応をすれば、ピンチをチャンスに変えることもできます」と強調する。

デロイト トーマツ リスクサービス
シニアマネジャー
亀井 将博 氏

CSIRTを設置し、情報開示を念頭に置いたインシデント対応を行う

第2回サイバーセキュリティセミナーに登壇した亀井氏は、はじめに過去の情報開示例を提示し、「起こったことそのものよりも、その後の情報開示で大きく評判を落としてしまったと考えられる企業がある」と切り出した。

たとえば建築基準法違反を犯したある企業では、“制限速度をわずかに上回ったという認識”という発言をして、非常に強い批判を浴びた。またサイバー攻撃によってユーザーの個人情報を漏えいさせてしまったある企業も“我々も被害者”という発言によって、強い批判を浴びた。

亀井氏は「このような対応を起こさないようにするためには、インシデント対応専任チームであるCSIRT(Computer Security Incident Response Team)を設置し、日常的活動、インシデント対応、事後活動という3つの取り組みを、諦めずに、しつこく、繰り返し行っていくことが重要です」と強調する。

実際の情報開示は、インシデント対応時の抑制、除去、回復の各段階に応じて進めていくことになる。

「インシデントが発生した時、企業が最初にするべきことは、頭を下げることではなく、被害者の方にいち早く通知することと、被害を拡大させないことです。そこでまず抑制の段階では、サービスを止めたほうがいいかの判断を下し、どのように情報を発信していくのかを定義した“ポジションペーパー”を作り、情報の拡散力を持つマスメディアやインターネットメディアの力を借りて告知します」。

次にインシデントの除去段階では、何が原因でこの事象が起こり、被害がどれぐらい出ているのか、さらに拡大する可能性があるのか、また再発防止にメドは付いているのかなどの項目が整理できた時点でお詫びと釈明を行う。これらの項目が整理できていない段階で会見を開いても、「単に頭を下げることしかできません」。

そして回復の段階では、再発防止策を策定して公表し、またサービス再開の告知も行う。ここで公表する再発防止策は「検証可能で現実味のあるものでなければ意味がない」という。

自社の発表に対して社会からどんな意見が出ているのか、その論調を把握する

抑制／除去／回復の各段階ではそれぞれ開示する情報も異なる。まず抑制段階における情報開示は、被害拡大抑制のためにサービスを停止するという案内や注意喚起が主なものとなる。そして情報開示後には、たとえばソーシャルメディアで自社の発表に対して社会からどんな意見が出ているのか、その論調を把握することが効果的だ。

「自社がインシデントの発生を公表していない段階にも関わらず、一部の人々が既に何らかの情報を知っていて、特定のメディアで議論が交わされていた、ということもありました。そういった投稿によって企業は情報開示の前倒しを迫られます。ソーシャルメディアの論調把握は、そういったことにも利用できるのです」。

次に除去の段階では、作成したポジションペーパーをベースに情報選定をして開示を行い、さらに開示した情報に基づくお詫びと釈明を行う。

「自社の現状と非常によく似た事象に見舞われた企業が、過去に存在することは少なくありません。その際にその企業がどんなお詫び文を出したのかは非常に参考になります。我々はメディアに提供されたお詫び文のデータベースを持っており、約2万件のデータを保有しています。こうしたものをご利用いただくことも可能です」。

さらに除去段階でもソーシャルメディアの論調把握は有効で、また記者会見で想定されるQ&Aを作成しておくことや、疑似記者会見を行うことも効果が高いという。

危機対応時の情報開示のやり方一つで、自社のピンチをチャンスに変えることもできる

そして回復の段階では、第三者委員会による調査や再発防止策の策定、サービスを再開する範囲の選定を行い、それらの告知を行う。回復段階でのありがちな失敗例としては、記者会見における不適切なスポークスパーソンの選定に加え、再発防止策が抽象的になってしまっているケースが挙げられる。たとえば再発防止委員会を設置するといっても、それで何がどう変わるのか、外部にはよく分からないことがある。また再発防止策の検証方法や検証期間を明示していなければ、自社の本気度を疑われることにもなり、社内的にも緊張感が薄れて検証自体がおざなりになり、同様の事案を起こしてしまう恐れがある。

「懸命に予防策を考えて発生確率を下げたリスクの発生は、考えたくないことです。しかし“努力して発生確率を下げたそのリスクが発生してしまう”という前提で準備をしなければなりません。直感的にでもいいし、数値的にでもいい。できるだけ多くの社内関係者を交えて、発生の可能性を低く抑えてはいるが、しかし一旦これば非常に深刻な影響を受けるリスクを再確認することが重要です」。

最後に亀井氏は「危機対応時の情報開示のやり方一つで、自社のピンチをチャンスに変えることもできる」と強調する。

「情報漏えいが起きることは企業にとって紛れもなくマイナスです。しかし適切な情報開示を行い、マイナスを上回るプラスの情報を提供することができれば、レピュテーションをいい方向に変えていくことができるかもしれません。実際にピンチをチャンスに変えた実例もあります。インシデントの進捗に即した情報開示と、それを意識した日頃からの準備が何よりも肝要なのです」。

※本記事は、2014年11月14日に掲載されたビジネス+ITからの転載です。

お問い合わせ先

Deloitte. トーマツ.

デロイトトーマツ リスクサービス株式会社
〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル
Tel:03-6213-1300　URL : www.deloitte.com/jp/dtrs