SUCCESS STORY

経営層自ら実施
事業継続や組織運営を踏まえたサイバーセキュリティインシデント演習

ANAホールディングス株式会社 https://www.ana.co.jp/group/
東京都、日本 | 連結従業員数41,225人 (2024年3月31日現在)
実施した演習:経営層向けセキュリティ演習

ANAホールディングス株式会社(以下ANAグループ)は、航空運送事業を行っており、NISCが指定する重要インフラ事業者に位置付けられている。ANAグループでは重要インフラを担う企業としてサイバーリスクも重視していることから、情報セキュリティ推進体制をグループ全体で立ち上げ、日常的に情報システムの機能向上や多層防御によるセキュリティ対策を講じてきた。

こうしたサイバーセキュリティ対策推進の一環としてANAグループでは、インシデント対応体制を組織している。今回演習実施を推進した「ANAグループCSIRT」はこのインシデント対応体制における中心的な役割を担うバーチャルチームだ。ANAグループCSIRTは、複数の部署のメンバーで構成されており、セキュリティイベントの発生時には会議体を設け、状況整理や対応方針の協議を行うなどの活動を行っている。さらに緊急時対応だけにとどまらず、セキュリティの予防段階における研修やマニュアル整備などの企画·運営も実施しており、今回の演習もそうした活動の一つである。

演習実施の背景

ANAグループCSIRTとしては、経産省のサイバーセキュリティ経営ガイドラインにも記載の通り、経営層の主体性や積極的な取り組みがセキュリティ推進において重要であるということを以前から認識していた。また近年のサイバー攻撃被害の事例を見ても、断片的な情報が飛び交う切迫した状況下で素早く高度な経営判断が求められる場面も少なくない。こうした背景から組織のトップ層が万が一の事態においても、混乱に陥ることなく対応できるようなセキュリティ演習実施の必要性を感じており、社内のIT部署などからも声が上がっていた。

そうした折、トレンドマイクロからの演習実施の提案を受けた。提案の中に経営層自らが限られた時間や情報、条件などの中でどのように危機対応判断を行うか、という実践的な意識啓発要素が含まれていた点や、事業継続と組織運営を踏まえた経営判断のポイントを演習前段の講義で伝え、経営層間の共通認識を醸成する企画が効果的であると判断し、依頼に至った。

実施効果:

- DX関連やリスク管理担当だけではなく、事業の中核を担う役員を含めた、トップマネジメント主体の演習実施
- サイバーインシデントに対する事業継続と組織運営を踏まえた意思決定や方針の認識合わせ

「経営層が自分事としてサイバーリスクを捉えることを重要視しました。サイバーセキュリティの専門家に事例情報などのインプットを受けつつ、意見を求められるという演習形態によって、DX関連やリスク管理担当だけではなく、事業の中核を担う経営層も高い緊張感をもって取り組めました」

ANAグループCSIRT
ANAホールディングス株式会社

演習内容

演習実施に向けてANAグループCSIRTでは約半年間、トレンドマイクロと定期的にミーティングを行い、演習の内容を調整した。多数の役員を集めた長時間の演習は困難である為、限られた時間内で高い成果を生み出せるよう入念な準備が必要だった。

今回の演習に参加する役員の立場はDXやリスク担当役員以外にも航空機運航を担当する役員など、幅広い担当領域の役員が集まる。担当領域の異なる彼らに「不測の事態における高度な判断を迫られる経験」をしてもらうことで、サイバーセキュリティと事業·役員自身の担当領域との関わりをいかに感じてもらうか、が焦点となった。

そこでまず、シナリオとして航空機の運航に影響がある事態を設定し、多くの役員の担当領域に関係するものとした。さらにシナリオの中で、実際に使用している部署名やシステム名称などを反映したり自社の従業員情報が危険にさらされる状況を想定したりなど、リアリティを感じさせる演習とすることに努めた。他にも、最新の脅威がもたらす状況を想定できるよう、サイバー攻撃を通じて段階的に脅迫が行われるようなシナリオを取り入れた。

こうしたシナリオの作成にあたってはサイバーセキュリティの動向に関する専門知識と自社の事情に合わせた柔軟な演習カスタマイズの両方が必要であり、トレンドマイクロと協力しながら効果的なシナリオを検討した。

演習の準備を振り返ってANAグループCSIRTのメンバーは「外部に演習を依頼することは、自社だけの目線でプログラムを作るよりも、他社事例などの知見をもつセキュリティの専門家企業と協力することで説得力のある演習ができるメリットがある」と述べた。

演習の際には、経営を踏まえたセキュリティマネジメントの知識を有する講師が登壇し、それぞれのフェーズでどのような対応を選択するか、経営層個人個人にその場で質問を行う形で実施することにより、過去の演習よりも緊張感をもって取り組ませることができたという。

今後の展望

今後について、ANAグループCSIRTのメンバーは「今回のような経営層への演習はこれからも定期的に実施していきたい。また今後はグループ全体での連携も重要視していることから、各グループ会社のメンバーも巻き込んだ演習など範囲を広げていくことを考えている」と述べた。昨今のサプライチェーン攻撃などの脅威を踏まえれば、自社の安全性を高めるだけでは事業へのサイバーリスクを低減することは難しい。ANAグループでは、より幅広い視野でグループ全体を含めた危機対応体制を向上していく予定だ。

詳細はこちらから

https://trendaisecurity.com/ja

TrendAI™ について

TrendAI™ は、トレンドマイクロのエンタープライズ向け事業部門であり、AIセキュリティのグローバルリーダーです。AIの包括的な可視化と統合セキュリティの提供を通じて、組織に確かな信頼をもたらし、イノベーションを推進するとともに、リスクを最小化します。

現在、世界185か国において大手企業や政府機関に採用され、アイデンティティ、インフラ、データに至るまで、組織全体を横断したセキュリティを提供しています。AI Fearlessly.

https://trendaisecurity.com/ja

参加者への効果

今回の演習の最も大きい効果としてANAグループCSIRTのメンバーはこのように述べた。「演習では、それぞれの役員からの意見や議論を通じて経営層の中でも意識統一が図れた点がよかった」

危機対応の中での意思決定には、リスクがつきものであり、高度な判断が必要となる。例えば、セキュリティインシデントの公表タイミング一つとっても、すばやい公表が常に正解というわけではなく、正確でない情報が誤解や混乱を招くリスクがあり、必要以上の損失につながってしまう可能性を含んでいる。

そうした中、社内でも事業継続性を優先するか、従業員の安全を優先するか、など、部署や個人によっても認識が異なる可能性が高い。時間との戦いを強いられるインシデント禍において重要なことは、事前にそうした危機的状況での優先順位について組織の方針が定まっている、ということである。

「経験に裏付けられた、公表情報では読み取れない攻撃者の意図や被害組織の実情など、表面的なものではなく胸に迫るお話が聞けた点がよかった」ANAグループCSIRTのメンバーは演習の講師がもたらした効果についても述べた。セキュリティの現場を詳しく知る専門家が伝えた情報が参加者のセキュリティに関する興味を促進できたという。

また実際の参加者アンケートでは、「サイバー攻撃を受けた時の企業側が想定しづらいシナリオが設定されており、かつ、複数の対応パターンが用意されており、短時間の演習としては、非常に効果的だったと思います」といったコメントや「実際のオペレーションに則したリアルな想定によるケーススタディで、世の中の動向も触れられつつ、改めて当社が狙われる場合の理由なども説明され、より自分ごと化するきっかけになった」といったコメントが寄せられた。社内にない知見や自分事と捉えやすい説明が受講者にとっても刺激になったことがわかる。