青い森のサイバーセキュリティ

令和３年９月
青森県警察本部保安課
サイバー犯罪対策室

夏休み後のセキュリティ確認！

休暇明けはセキュリティ侵害の有無を再確認

内閣サイバーセキュリティセンター(NISC)は７月21日、重要インフラ事業者などに向けて「夏期休暇等に伴うセキュリティ上の留意点について」を公開し、夏期休暇やオリンピック期間中の情報セキュリティの確保について注意喚起を行いました。

一方、休暇期間中はサーバーの監視体制が弱まり侵害に気づくのが遅れたり、休暇明けにおいては、休暇期間中にサーバーに蓄積された大量のメールが、従業員端末のウイルス対策が更新される前に一斉に受信され、ランサムウェア等の紛れ込みに気づきにくくなるなど、通常業務への復帰に伴いインシデントの発生、もしくはインシデントの発覚率が高まります。

こうしたことから、休暇明けは、各種サーバーログのチェックや従業員端末のウイルスチェックの強化など、セキュリティリスクについて十分に確認を行いましょう。

【NISC｜夏期休暇等に伴うセキュリティ上の留意点について】
https://www.nisc.go.jp/active/infra/summer20210721.pdf

１．テレワークに関するセキュリティリスク
２．ランサムウェアに関するセキュリティリスク
３．新たに確認された脆弱性に関するセキュリティリスク
４．東京2020大会に関するセキュリティリスク
５．長期休暇に伴うセキュリティリスク

【休暇明けにすべき確認】

・業務開始後早期のウイルス対策の更新
・休暇期間中に報告された事案への対応
・ログのチェック
・ネット機器の脆弱性情報の確認　など