ORCA CO., LTD.
3F X's Bldg., 26-22, Higashi-Ohi 5chome, Shinagawa-ku Tokyo, Japan
TEL:81-3-3471-8898　FAX:81-3-3471-8899　E-mail: systemdiv@orcajpn.co.jp

ORCA REPORT　船舶におけるランサムウェア攻撃の対策

・初めに

先日、KADOKAWA 社のサーバがランサムウェア（身代金要求型マルウェア）の攻撃を受けたことが報道されております。この攻撃により同社の業務サーバ内の大部分の情報が流出し、業務が停止するなどの被害が発生したとのことです。また、2024 年だけでも、日本生命、クボタ、公文などの大企業がランサムウェアによって個人情報流出などの被害を受けております。

ランサムウェアによる攻撃は世界中に広がっています。船舶においてランサムウェア被害を受けたという報告はまだありませんが、現実的にありうると想定して警戒と対策を行うべきと考えます。

ここでは船舶ネットワークにおいて、ランサムウェア攻撃の対策についてまとめましたのでご参照ください。

・結論

まずランサムウェア対策に関する結論を以下の通りまとめます。

1)　これだけやっていれば 100%安心という対策は存在しない。
2)　攻撃の可能性を下げる対策としては、Anti-Virus、監視システム、ネットワーク設計、ユーザー教育など複合的な対応が必要。
3)　攻撃を受けてしまった場合の被害の最小化対策として、「重要データの洗い出しと運用の変更」「バックアップの遂行」が重要。

・ランサムウェアとは

ランサムウェアは「身代金要求型のマルウェア（悪意のあるプログラム）」です。実行されるとネットワーク内のデータを暗号化し、場合によっては外部に送信する機能を持っています。
一度ランサムウェアに感染するとネットワーク内のデータが利用できなくなり、業務上支障をきたします。暗号化されたデータを元に戻すには暗号鍵が必要であり、ランサムウェアの作者はこの暗号鍵の対価として金銭（身代金）を要求します。また、データを流出されては困るような情報（個人情報や企業機密）が含まれる場合は、これを他に流出すると脅迫することでも身代金を要求します。

・侵入経路

ランサムウェアの侵入経路は「メール」「インターネットダウンロード」「VPN からの侵入」「ユーザーによる持ち込みインストール」などの多岐にわたります。最近では VPN 経由での侵入が多いと報告されています。

・防御が難しい理由

ランサムウェアは定形的なコンピュータウィルスプログラムと違い、特定のネットワークを狙い撃ちにする「カスタマイズされたプログラム」であるため、定義ファイル型の Anti-Virus では検出しづらい特徴があります。また、アルゴリズムを検出するタイプのアンチマルウェアであっても、その動きを必ず検出できるとは限りません。
また、多くのランサムウェアはユーザーが自ら実行してしまうような作りになっています。ランサムウェアはそのユーザーの権限を持って実行されるため、そのユーザーに許可されたアクセス範囲のデータがすべて攻撃対象になってしまいます。

監視系の防御システムがあれば、ランサムウェアの動作を検出して警告することが可能です。
しかし警告されるまでの間、起動してしまったランサムウェアはネットワーク内のデータをどんどん暗号化あるいは外部流出させてしまいます。
すなわち、実行に気づいたときにはもう遅いということです。

・もたらす情報被害

ランサムウェアがもたらす被害は下記の三つの要因に分類することができます。

1) 可用性に対する被害
データが暗号化されると、必要な時に必要な業務データが使えなくなります。例えば PSC 直前に過去の SMS 記録にアクセスできない事態を想像してください。
2) 完全性に対する被害
ランサムウェアはデータを暗号化するだけでなく、内容を書き換えたり、一部削除することがあります。今そこにあるデータの信頼性がなくなることは、(1)の可用性と同じ被害を引き起こします。
3) 機密性に対する被害
ランサムウェアはデータを外部に流出させます。その内容が企業秘密であれば
企業ノウハウの逸失はそのまま会社のダメージになりますし、個人情報や他社の機密情報だった場合は賠償責任を問われることになります。

・被害にあった場合

言うまでもありませんが、犯人に接触して身代金を払うことは避けるべきです。確実に復旧される保証はありませんし、国によってはテロリストに資金援助した罪に問われる可能性があります。
SMS マニュアルに基づき緊急対応チームを招集し、情報を収集して専門家のアドバイスを受けてください。場合によっては対外的な公表を行う必要もあります。

・攻撃の可能性を下げるための対策

上記の通りランサムウェアを防止することは大変難しいです。とはいえ攻撃を受ける可能性を少しでも下げるため、以下の一般的な対策は正しく実施されるべきです。

メール運用	ドメインに対してホワイトリスト型の運用をするとそこが侵入口になります。ホワイトリスト運用は止めるべきです。
Anti-Virus の運用と更新	既知のランサムウェアであれば防止できる可能性があります。
OS やソフトウェアの更新	OS 起因のセキュリティホールをふさいで侵入の可能性を低くすることができます。
ネットワークの分離	VPN アクセスによる被害範囲を狭くするため、船内ネットワークは機能別に分離することが有効です。ランサムウェアの攻撃可能範囲を狭くすることができます。
ユーザーの教育	会社に承認されないソフトウェアを実行させることは予期しないインシデントを引き起こす可能性があります。全てのマルウェアはプログラムであり、ユーザーが実行させなければ害は発生しません。よって、ユーザーの教育が最も大事です。

・攻撃を受けた後の被害を最小化する対策

1) 機密性に対する対策
ランサムウェアは身代金型のマルウェアであり、ネットワーク内にあるデータの機密性が高ければ高いほど身代金を要求しやすくなります。
よって、海運業界においては、各船にあるデータの機密性についてリスクアセスメントを実施しておく必要があります。
一般論として、船舶内にあるデータには損害賠償を発生させるような機密性の高いデータは

それほど含まれておりません。しかしながら他社の機密情報を保持しているケースには十分ご注意ください。それぞれのデータの性質を把握しておくことは対策の策定に役立ちます。

機密性の低いデータ	内容を把握しておき、流出のリスクを許容するのが現実的です。
機密性の高いデータ 及び 流出すると損害賠償の 対象となるデータ	全員からアクセスできる共有フォルダではなく、個人フォルダ、または物理的に切り離した別ドライブで運用すると流出を防げます。 また、データをパスワード ZIP にしておくと、万が一流出しても内容まで流出する可能性を低くできます。もちろんパスワードはサーバ内に記録してはいけません。

2) 完全性、可用性に対する対策
こちらは定期的にバックアップを取得するシステムが動いていれば、ほとんどの場合安全に復旧可能です。暗号化されてしまったデータは廃棄し、バックアップデータを戻すことで業務を継続できます。バックアップは Daily、Weekly などと複数世代保持しておくとなお安全です。また、バックアップドライブはネットワークから直接アクセスできない構造にしておくことが有効です。そうすればバックアップデータが暗号化されることを防止できます。

・まとめ

1) 結論としてランサムウェアの攻撃を完全に防げる方法は存在せず、一般的なセキュリティ対策を積み重ねるしかありません。

2) 攻撃を受けてしまった場合、情報漏洩の被害を最小限にするために、船内データの洗い出しとリスク評価を行ってください。リスクの高いデータは共有フォルダにおかない、パスワード ZIP にするなどの対策を行ってください。

3) 情報の可用性完全性の被害を最小限にするにはバックアップが非常に有効です。各船のバックアップシステムがどのようになっているか、また有効に機能しているかをぜひこの機会にご確認ください。*

＊弊社の設定した標準システムだと、バックアップは Daily と Weekly の 2 世代で、NAS とは別のドライブにバックアップされる仕組みになっています。

この他、ご不明の点がございましたらお気軽にご質問ください。
今後とも弊社の N-OASYS サービスをよろしくお願いいたします。

文責： 2024/07/23 株式会社オルカ 張