Deloitte.
デロイト トーマツ

ライフサイエンス＆ヘルスケアインダストリー
日本語版：2023年8月

発生は時間の問題

ヘルスケア業界における
ランサムウェア攻撃への対処

目次

世界のヘルスケア業界で、近年ランサムウェア攻撃が急増中

2022年、米国のヘルスケア施設は平均して一週間に1,410件のサイバー攻撃を経験した。この数字は2021年に比べて86%増加した。[1]一方、カナダでは、国内のランサムウェアの被害者の半数が医療など重点分野の企業であった。[2] 同様に、欧州の病院や医療ネットワークに対するサイバー攻撃は2020年に47% 増加した。[3]

サイバー犯罪エコノミーがこのような増加の要因である。サイバー犯罪は「濡れ手に粟」のビジネスであり、その収益額は毎年1兆5000億ドルを超えている。

標的への攻撃コストの大まかな平均値が0.0004ドルから400ドルまでに収まる点を考慮すると、信じられない額の利益が出ていることになる[4]。

また、およそ半数のランサムウェア攻撃はデータ侵害[5]を伴う。つまりランサムウェアは、年間利益約1600億ドルの個人データ販売と年間利益約10億ドルの身代金[6]の二つの大きな誘因を有する、サイバー犯罪者にとっては人気の攻撃手段なのだ。

院内ネットワークやヘルスケアネットワークが攻撃対象となりやすいため、上記2つは、ヘルスケア業界が特に被害を受けやすい分野でもある。

これらのネットワークは患者のセンシティブPII (個人を特定できる情報) 、処方歴、生命保険から組織の従業員、財務、知的財産に関する情報まで、広範囲におよぶ貴重なデータの宝庫だ。これらの多くは長期間にわたり保存され、販売だけでなくID盗難、恐喝、詐欺など関連犯罪へ容易に転用される。

近年の世界的なパンデミックでサイバー犯罪の新たな攻撃機会が生まれたことが事態の複雑化を招いている。ヘルスケア業界における仮想環境への急速な方向転換は、サイバーセキュリティコントロールの重大な欠陥を浮き彫りにした。とりわけ、ずっと昔にカスタマイズされたシステムや、現状のようなコネクティッド状態を想定して作られていない、複雑なIT環境にあるままの重要な情報が脅威に晒されているのは顕著である。加えて、セキュリティチームの人材不足と潤沢ではないサイバー予算に鑑みれば、ヘルスケア業界がサイバー犯罪者の標的となったのは当然であろう。

このような状況に照らせば、不幸にもサイバーセキュリティ侵害はほぼ不可避である。しかし、幸運なことに組織の攻撃対象としての魅力を減らし、攻撃を受けた際の被害を抑えるためにできることはある。重要なのは、今日の洗練されたサイバー攻撃主体に対峙する際に、効果的な防御策と攻撃から自信をもって回復できる能力を備えておくことだ。

本稿では、急速に進化するサイバーセキュリティランドスケープに対して、医療組織が後れを取ることなく攻撃に備えるにはどうすればよいかを探る。

防御戦略の策定

サイバーセキュリティの敵対者はもはや個人のハッカーではなく、高度に組織化されたサイバーギャング、政府の支援を受けた攻撃主体や洗練された犯罪集団であるということに、既にほとんどの組織が気づいている。

サイバー犯罪者の攻撃は、さまざまな方法でさまざまな場所から発される一方で、その目的は通常、可能な限りのダメージを標的に与え身代金（ランサム）を払わせることで一致している。

サイバー犯罪集団は資金や資源を活用して多様な手段でランサムの支払いをさせようとする。従業員や請負業者に声をかけ、報酬と引換えに代わりに組織ネットワークに内部からアクセスさせるのは、ヘルスケア業界への典型的な攻撃手法の一つである。

また、基本的なウェブアプリケーションを狙い、サードパーティへの攻撃を介して標的の組織システムに侵入する手法もある。[7]

どの方法であれ、一度医療組織の境界線がサイバー犯罪者によって突破されると、93% [8]の場合においてその先のローカルネットワークへのアクセスは遥かにたやすくなる。

そこからは、重要システムをシャットダウンしたり、重要な情報やデータへのアクセスをブロックしたり、ネットワークに接続されている救命・生命維持装置をハッキングし、そのアンロックのために身代金を要求することも可能になる。

こうした攻撃は、データプライバシーの侵害はもちろん、入院期間の長期化、医療処置や検査の遅延、ひいては患者の死亡といった破滅的な結果をもたらす可能性がある。[9]

したがって、医療組織は、境界線侵害を抑止するためにはサイバー防衛能力を強化して、自組織を狙った攻撃の費用対効果を下げることを目指すべきである。そのために理想的なのは、境界線市街に関する5つの主要分野に焦点を当てることだ (p .04参照)。

境界線侵害の抑止策

ユーザーのサイバーセキュリティ意識の向上
一般にユーザーは組織防衛の第一線を形成する。対象者を絞った研修や啓発活動、またユーザー集団のパフォーマンスの継続的なモニタリングを通じて、ハッカーの境界線侵入の難度を相当程度上げることができる。

技術的な攻撃対象領域の縮減
ハッカーは標的組織の中でも最も脆弱性が高い箇所を好んで攻撃するため、脆弱性管理、パッチ適用、システムハードニング、そして エンドユーザセキュリティ強化（例：ブラウザ分離）予防的に行い攻撃対象領域（アタックサーフェス）を減らすことが不可欠だ。

検知率の向上
サイバーランドスケープの進化が止まることはないため、ストレージ機器での疑わしいファイルアクティビティなど、異常動作や攻撃の兆候を検知できるよう組織環境を常に監視する必要がある。

水平移動の制限
ハッカーによるシステムへのアクセスがあった場合、その影響を最小限に抑えたいと考えるのは当然のことだ。IDや特権アクセス管理などのゼロトラスト原則とネットワークセグメント化を実装することで、ネットワーク内におけるハッカーの水平移動とそれに伴う影響の拡大を制限できる。

分離と区画化
影響を受けたシステムの隔離が早ければ早いほど、迅速に関連する損傷の封じ込めが可能である。インフラ設計段階で区画化機能を積極的に組み込んでいればこうした隔離は容易になる。

“境界線侵害を抑止するためには、サイバー防衛能力を強化し、攻撃の費用対効果を下げることを目指すべきである。”

レジリエンスを発揮し、重要な業務を維持

強固な防御戦略と同様に、侵害への組織的対応能力もサイバーセキュリティの重大要素である。

短い反応時間で直ちにランサムウェア攻撃に対応できる能力は、レジリエンスを向上させ、脅迫に遭う可能性を低下させ、誰かの命を救うことにさえ繋がるかもしれない。

つまり、対応と復旧能力を強化し、事前に所管チームが対応方法を把握できている状態を作り出すのが肝要である。

対応および復旧能力の向上施策

組織単位の準備と調整
侵害発生時に組織が対応に向けて滑らかに動き出すためには、前もって機能横断的な危機管理・対応チームを組成し、組織単位で復旧に関する机上訓練、実践演習、ストレステスト、そして過去事例の事後分析を重ねておくことが有用である。

バースト容量の管理
進行中の攻撃に効果的に対応するには余剰部分から不足部分へのリソースの再割り当てが必要である。
物理的に保有するものからサードパーティーサービスまで、あらゆるリソースで同じことが言える。

復旧計画の策定
技術的・非技術的な計画とプレーブックを備えておくことで、組織は段階を追って復旧を進めることができ、事業運営上の重要度に応じてオペレーションの優先度を決定することができる。
復旧時の優先順位と順番を決めるには、バリューチェーンの全体像を隅々まで理解しておくことが不可欠である。

効果的なコミュニケーション
侵害が起きた際、コミュニケーションの経路や手順は明確でなければならない。また、全体を通じて透明性を確保しつつ、関係者に落ち着いて行動することを繰り返し呼びかけることも忘れてはならない。内部と外部の双方の要求の応えるような周到なコミュニケーション計画を練れば、冷静に、また集中して復旧を進めることができる。

侵害されたデータの量と機密性に応じて、患者や当局とのやり取りが発生しうるため、医療組織にとってコミュニケーションはとりわけ重要な項目である。

復旧のためのツールの準備
侵害を受けたインフラを再構築する前に、適切なツールとマテリアルを手元に揃えておかなければならない。イミュータブルなデータ、分離済みの復旧環境、復旧オペレーションのオーケストレーションが挙げられ、これらはすべて復旧作業の大幅な時間短縮に役立つ。

自信をもって復旧を実施

医療組織は、絶えず変化するサイバー脅威ランドスケープにも迅速に適応していかねばならない。

すなわち、サイバー攻撃を検知して重要資産を保護すればいいというわけではなく、侵害発生時のレジリエンスに磨きをかける必要がある。

状況に応じて、被害を受けたシステムやデータ資産の修復をすることもあれば、機能停止が長期に及んだ場合に備えて業務継続計画を立てることもあるだろう。

どんな状況においても、医療組織には求められているのは、患者を守るための基礎として重要システムの稼働を維持することである。

脅威ランドスケープの変化につれて重要システム稼働の維持は困難になるため、準備の高度化は必須となる。

組織を狙った攻撃を未然に防ぐには、ミッションクリティカルなサービスを特定し、保有する様々なシステム間の相互作用を理解し、定期的なトレーニングを受け、回復の成熟度を継続的に向上させる必要がある。

お問合わせ先

注釈

1 *https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022*

2 *https://globalnews.ca/news/8427930/canadian-health-energy-sectors-increasingly-targeted-by-ransomware-attacks/*

3 *https://www.balcanicaucaso.org/eng/Areas/Europe/Cyber-attacks-are-growing-in-the-European-Union-21652*

4 *https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf*

5 *https://www.kroll.com/en/insights/publications/cyber/ransomware-attack-constitute-data-breach*

6 *https://www.techrepublic.com/article/cybercriminals-raking-in-1-5-trillion-every-year/*

7 *https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf*

8 *https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=70ea31106b61*

9 *https://www.ibm.com/thought-leadership/institute-business-value/report/medical-device-security*

縣　和平
Partner - Deloitte Tohmatsu Cyber LLC
Life Science & Health Care Sector Lead
kazuhira.agata@tohmatsu.co.jp

Davies, Ari
Partner - Deloitte Tohmatsu Cyber LLC
Attack & Respond Lead
ari.davies@tohmatsu.co.jp

野見山 雅史
Partner - Deloitte Tohmatsu Cyber LLC
COO & CISO Transition Lab Owner
masafumi.nomiyama@tohmatsu.co.jp

Deloitte.
デロイト トーマツ

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited