ivanti

2023 Cyberstrategy Tool Kit für internes Buy-In

Wie Sie Budgets gewinnen und Stakeholder beeinflussen, die Bedeutung Iher Cybersicherheitsstrategie erklären

in collaboration with

CSW Cyber SecurityWorks

Vorwort

Willkommen, Fremder!

Dieses eBook wird Ihnen und Ihrem Team die Cyberdefense-Strategie für das nächste Jahr auf eine Weise erläutern, die jeder in Ihrem Unternehmen verstehen, finanzieren und befolgen kann.

Wenn Sie am Ende angelangt sind, wird dieses eBook Folgendes ermöglichen:

1. Bieten Sie den Nicht-InfoSec-Mitarbeitern Ihres Unternehmens eine leicht verständliche, kontextualisierte Zusammenfassung der wichtigsten Bedrohungsakteure und ihrer Angriffsmuster für das Jahr 2022 und stellen Sie den panischen Schlagzeilen, die die Endbenutzer in den Medien sehen, Ihre strategischen Sicherheitsempfehlungen gegenüber.

2. Demonstrieren Sie genau die proaktiven Sicherheitsmaßnahmen, die Sie schon immer umsetzen wollten –und die jeder nutzen kann! – und wie diese verheerenden Angriffe im Keim erstickt hätten.

3. Helfen Sie allen Beteiligten und Endnutzern, das Gefühl zu haben, dass sie dazu beigetragen haben, größere Sicherheitsverletzungen und Angriffe zu verhindern, indem sie einfach das umsetzen und befolgen, was Sie seit Jahren von ihnen verlangen.

Wir möchten Ihnen helfen, Ihr Unternehmen im Jahr 2023 zu schützen – aber nicht durch den gleichen reaktiven „Patch the Headlines“-Ansatz, der Ihren Posteingang alle zwei Monate mit panischen Anfragen überflutet.

Ihr Team ist ausgebrannt, weil es versucht, diesen Ansatz zu verfolgen.

Ihr Unternehmen ist ausgebrannt!

Nutzen Sie stattdessen dieses eBook-Toolkit als ersten Schritt, um das „Warum“ hinter Ihrer Verteidigungsstrategie - nicht nicht nur das „Was“ – auf eine Art und Weise, die auch Menschen außerhalb InfoSec verstehen können. So können Sie die

Zeigen Sie das „Warum“ hinter Ihrer Cyberdefense-Strategie – nicht nur das „Was“.

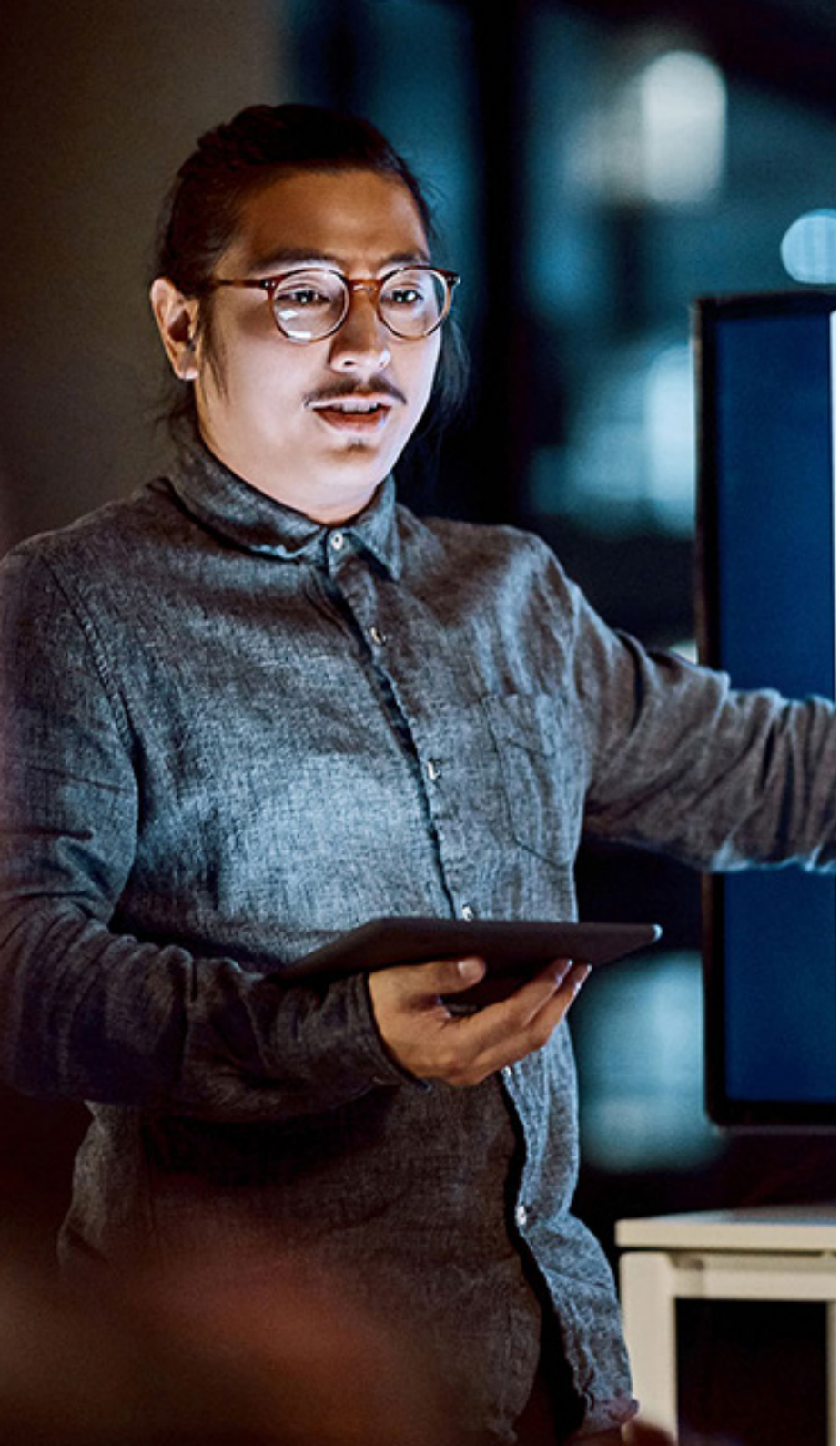
Grundlage für die Investitionen legen, die nötig sind, um Cyberangriffe zu stoppen, bevor sie passieren.

Wir wünschen Ihnen viel Glück, Fremder. Möge dieses Handbuch Ihrem Team helfen, die Ressourcen, die Arbeitskraft und die Zeit zu bekommen, die es braucht, um das zu tun, was es am besten kann: die Sicherheit Ihres Unternehmens im nächsten Jahr – und darüber hinaus zu gewährleisten.

Erwecken Sie Statistiken zum Leben durch die wahren Geschichten, die wir hier zusammengetragen haben, von Unternehmen wie das ihre, die von verschiedenen Cyberkriminellen mit einzigartigen Motiven und Einbruchsmethoden angegriffen wurden.

Gehen Sie über die MITRE-Analyse und die CVE-Kritikalität hinaus, um den Beteiligten zu zeigen, wie kleine Investitionen in „Sicherheits-Extras“ dazu beigetragen haben, verheerende reale Angriffe zu verhindern, und zwar in einer Sprache und einem Format, das auch Menschen außerhalb der InfoSec-Welt verstehen können.

Belegen Sie, wie ein paar Monate zusätzliche Zeit und Ressourcen Ihrem Team die Möglichkeit geben, unternehmensübergreifende Patches oder Abhilfemaßnahmen zu testen und einzuführen, ohne den regulären Geschäftsbetrieb zu unterbrechen ... und bevor Kriminelle Ihre Systeme ins Visier nehmen könnten.



Inhalt

Das Verteidigungsverzeichnis:
Wie Sie Ihre Mitarbeiter wappnen und Ihr Team unterstützen

ivanti CSW Cyber SecurityWorks

Bevor wir dazu kommen, wen wir in den nächsten zwölf Monaten in unseren Netzwerken bekämpfen, müssen wir damit beginnen, wie Ihr Unternehmen ihre Verteidigung vorbereiten sollte – und das schließt die Tools und Taktiken ein, die Sie implementieren wollen, bevor ein größerer Einbruch stattfindet.

In der Tat könnte jede dieser ausgewählten Lösungen praktisch jeden Angreifer, den wir für dieses Tool Kit ausgewählt haben, auf die eine oder andere Weise abwehren.

Wenn alle Beteiligten ein klares Verständnis der möglichen Verteidigungsmechanismen haben, die Ihr Team einsetzen könnte – wenn es Zeit, die Zustimmung der Führungskräfte und die entsprechenden Ressourcen hat – dann werden wir genau aufzeigen, wo und wie diese Techniken einige der häufigsten und ruchlosesten Cyberangriffe des Jahres 2022 hätten verhindern können.

Jede Cyberverteidigungstaktik umfasst:

- Zeit bis zur Funktionsfähigkeit und Kosten.
- Eine vereinfachte Beschreibung dessen, was das Verteidigungstool ist.
- Eine Erklärung, warum es funktioniert, bestimmte Arten von Cyberangriffen abzuwehren.
- Ein „Wappnen Sie Ihre Mitarbeiter!"-Spickzettel, um häufige Einwände interner Stakeholder zu überwinden und das Gespräch von „Warum brauchen Sie das?" auf „Wie können wir helfen, das zu bezahlen und umzusetzen?" zu verlagern.

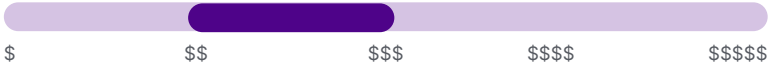
Das Verteidigungsverzeichnis:
Wie Sie Ihre Mitarbeiter wappnen und Ihr Team unterstützen

In diesem Abschnitt

Anti-Phishing

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Der Begriff „Anti-Phishing“ bezieht sich häufig auf eine Reihe von Tools, die Hacker daran hindern sollen, Benutzer dazu zu verleiten, auf bösartige Links zu klicken oder bösartige Dateien herunterzuladen, und zwar über verschiedene Plattformen, Geräte, Browser, Anwendungen und Textnachrichten hinweg.

Wie es hilft, sich zu verteidigen

Der Mensch ist nicht perfekt! Sollte es einem Hacker gelingen, jemanden dazu zu verleiten, auf einen Link zu klicken oder einen Dateidownload zu starten, können diese Tools verhindern, dass eine bösartige Aktivität tatsächlich stattfindet.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Haben wir nicht einen Filter für Spam-Nachrichten? Warum sollten wir uns etwas anderes besorgen?

Ja, es gibt kostenlose Tools für einige Browser und E-Mails. Sie sind jedoch nicht auf allen Plattformen verfügbar, und die Vorfälle nehmen zu, da Mitarbeiter zunehmend private Geräte für berufliche Zwecke nutzen.

Warum dauert die Implementierung von Anti-Phishing so lange, nachdem wir es gekauft haben?

Listen Sie jedes Betriebssystem, jeden Gerätetyp, jedes Netzwerksystem, jeden Browser und jeden anderen Endpunkt auf, den Ihre Anti-Phishing-Lösung abdecken muss. Das sollte ausreichen, um zu verdeutlichen, warum es nicht sofort geht!

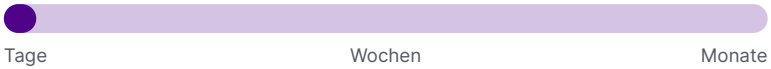
Warum sollten wir so viel für diese Tools bezahlen, wenn es auch kostenlose Versionen gibt?

Die höheren Kosten für robustere Anti-Phishing-Tools sind in der Regel auf die verschiedenen Plattformen und Geräte zurückzuführen. Das Hacken von Anmeldedaten durch Phishing ist eine gängige Taktik von fast allen Angreifern, unabhängig von ihrer eigentlichen Motivation.

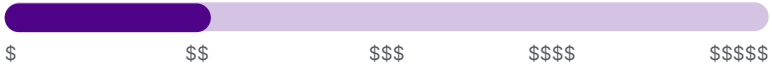
Anti-Phishing-Tools könnten also eine der einfachsten und billigsten Methoden sein, um teure Cybersecurity-Verstöße zu verhindern!

Antivirus / Antimalware

Zeit bis zur Funktionalität



Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Dies ist die grundlegendste aller Cybersicherheitslösungen, die einen umfassenden Schutz und eine allgemeine Abschreckung vor einfachen Eindringversuchen bietet.

Wie es hilft, sich zu verteidigen

Im Grunde genommen sind Viren- und Malware-Schutz das Nötigste, was jedes Unternehmen implementieren sollte – nur um die einfachsten oder opportunistischsten Bedrohungen zu blockieren und abzuwehren.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Warum sollten wir mehr Geld dafür ausgeben, wenn wir bereits „kostenlose“ Angebote von Anbietern haben?

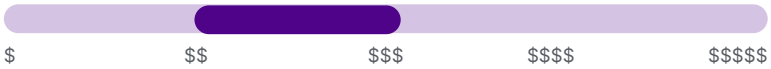
Wenn die kostenlose Version den Computer verlangsamt oder allgemein Probleme beim Betrieb verursacht, können Sie den Wechsel zu einer besseren Antiviren- oder Antimalware-Lösung rechtfertigen.

Wenn die Auswirkungen auf den Betrieb extrem genug sind, können Sie argumentieren, dass die kostenlose Software ihren Preis nicht wert ist. Ihre Stakeholder werden wahrscheinlich applaudieren, wenn Sie ein neues Antivirus- oder Malware-Tool beschaffen.

Anwendungskontrolle

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Tools zur Anwendungskontrolle erlauben nur bestimmte Anwendungen innerhalb der geschützten Umgebung. Diese Kontrollen sind typischerweise in stark regulierten oder unternehmensnahen Organisationen zu finden.

Wie es hilft, sich zu verteidigen

Indem nur Anwendungen oder Software von einer bereits überprüften „Whitelist“ von Anbietern zugelassen werden, verhindert die Anwendungskontrolle, dass unbekannte Payloads, die Malware und Trojaner verstecken, versehentlich von einem Mitarbeiter heruntergeladen werden - insbesondere solche ohne Zertifikate.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Warum sollten wir für die App-Kontrolle bezahlen? Wir haben bereits diese anderen Benutzerkontrollen!

Natürlich arbeiten alle Kontrollinstrumente zusammen und bauen aufeinander auf, um die bestmögliche Cyberabwehr zu gewährleisten.

Wenn Sie jedoch speziell für die Anwendungskontrolle budgetieren wollen, können Sie dem Stakeholder, der nicht aus dem Bereich InfoSec kommt, sagen, dass die Anwendungskontrolle dem Unternehmen Geld einsparen kann, indem die Anwendungsnutzung überwacht und ungenutzte „Shelfware“ eliminiert wird.

Wenn Sie das tun, kann ich die Anwendung XYZ, die ich für meine Arbeit brauche, nicht ausführen!

Dies ist ein weiterer Fall, in dem eine proaktive Kommunikation mit allen Stakeholdern Ihrer Nicht-InfoSec-Abteilung von entscheidender Bedeutung ist.

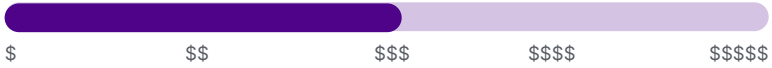
Erstellen Sie eine umfassende Liste der Anwendungen, die derzeit von allen Abteilungen genutzt werden - und entdecken Sie die Anwendungen, für die sie persönlich als „Schatten-IT“ bezahlen, wenn Sie können. Überprüfen Sie dann im Rahmen Ihres Whitelisting-Prozesses, dass jede App auf dieser Liste keine Sicherheitsbedrohung darstellt, damit der Geschäftsbetrieb ohne nennenswerte Unterbrechungen weiterlaufen kann.

Gestalten Sie dann den Prozess für die Beantragung einer neuen App, die der geschützten Umgebung hinzugefügt werden soll, so schmerzlos und schnell wie möglich, während Sie gleichzeitig sicherstellen, dass jede Anfrage von mindestens einem menschlichen Auge geprüft wird. Wenn Sie diesen Prozess vollständig automatisieren, könnten Hacker dies möglicherweise ausnutzen und heimlich die Erlaubnis für ihre eigenen Aktivitäten erteilen.

Verwaltung der Konfigurationen

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Einstellungen, Ports, Protokolle – all dies sollte bei der Konfigurationsverwaltung berücksichtigt werden, um sicherzustellen, dass das gesamte System eine sichere Basis hat. Zum Konfigurationsmanagement gehört auch, dass alle Artikel, für die Sie bezahlen, auf den richtigen Geräten landen und auch genutzt werden!

Wie es hilft, sich zu verteidigen

Häufig offene Ports und Konfigurationen sind Angreifern öffentlich bekannt. Das Festhalten an Standardeinstellungen oder nicht mehr unterstützten Versionen schafft erweiterte Angriffsflächen.

Die Konfigurationsverwaltung kann auch die gesamte Sicherheitstechnik unterstützen, indem sie sicherstellt, dass andere Sicherheitsprogramme nicht vergessen werden oder auf Geräten und in Umgebungen nicht richtig eingerichtet sind.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

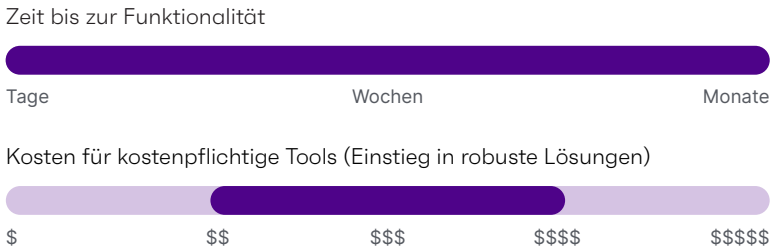
Warum müssen wir Konfigurationsmanagement kaufen?

Für kleinere Unternehmen ohne hohe regulatorische Hürden ist die Kosten-Nutzen-Analyse möglicherweise zu sehr auf die Kostenseite gekippt, als dass sie wirklich einen Wert für Konfigurationsmanagement-Tools sehen. Es kann auch ein kostenintensiver, manueller Aufwand sein. Stellen Sie also sicher, dass das von Ihnen gewünschte Tool nicht zu einer administrativen Belastung für Ihr Team wird.

Wenn es jedoch richtig gemacht wird, kann das Konfigurationsmanagement Ihrem Unternehmen helfen, Geld zu sparen, indem es sicherstellt, dass Technologieinvestitionen, die in allen Abteilungen getätigt wurden, auch tatsächlich installiert werden.

Gerätehygiene und -management

einschließlich Asset Discovery und Reconciliation



Beschreibung

Für dieses Verteidigungsverzeichnis definieren wir die Gerätehygiene- und Verwaltungslösung als das Tool oder die Tool-Suite, die erforderlich ist, um kontinuierlich Bedrohungen in jedem Endgerät, jeder Hardware und jedem Software-Asset in unserer Umgebung zu finden, aufzulisten, zu überwachen und darauf zu reagieren. Aus Sicherheitsgründen sollten die Lösungen auch alle direkten Abhilfemaßnahmen oder Aktionen, die im Falle eines identifizierten Eindringlings erforderlich sind, erleichtern oder integrieren.

Wie es hilft, sich zu verteidigen

Sie können nicht absichern, was Sie nicht kennen. Eine Cybersicherheitslösung erfordert eine robuste, dynamische und automatische Erfassung jedes Endpunkts in einem geschützten Netzwerk, da herkömmliche Geräteüberprüfungen nur zu dem Zeitpunkt genau sind, an dem die Erkennung abgeschlossen wurde. Asset-Erkennungsfunktionen unterstützen Hygiene- und Verwaltungsprogramme, indem sie nicht erfasste Geräte zum Schutz aufspüren ... und möglicherweise als potenzielle Eindringlinge, die sich als „nur ein weiterer Laptop“ im Netzwerk tarnen.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Wir haben ITAM – warum brauchen wir mehr?

Ein reguläres ITAM-Tool überwacht in der Regel nur die Geräte und Assets, die es zu finden erwartet, und zwar anhand von Kaufprotokollen und aktiven Verzeichnissen. Erinnern Sie diesen Stakeholder daran, dass das, was Sie nicht sehen oder noch nicht gefunden haben, das größte potenzielle Risiko für die Beeinträchtigung des regulären Geschäftsbetriebs darstellt.

Durch den Abgleich von Active Directory, Beschaffung, Endpunktmanagement und Endpunktprojektionssystemen entgehen Ihnen möglicherweise immer noch 20-30 % der Assets, die Ihr Unternehmen schützen sollte – ganz zu schweigen von den Geräten, die Hacker oder Angreifer einführen könnten, oder den Malware-Nutzlasten, die von nicht erfassten BYOD-Programmen stammen.

Warum für ein Upgrade bezahlen?

Mit zunehmender Größe eines Unternehmens wächst die Anzahl der Geräte schnell über die Möglichkeiten einer billigeren Option hinaus. Und einzelne Projektbeschreibungen werden sofort nach ihrer Fertigstellung abgebaut.

Außerdem sollten Sie bedenken, dass die meisten kostenlosen Tools, die in Software-Suites enthalten sind, nur selten eine dynamische Asset-Erkennung beinhalten, die unbekannte oder nicht erfasste Geräte erkennt, wenn sie in die Umgebung eindringen oder sie verlassen.

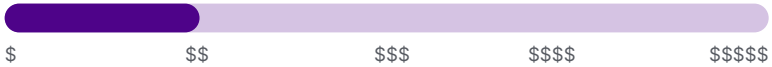
Für die Sicherheit ist die Erkennung von Assets ein entscheidendes Puzzleteil, nicht nur ein „Nice to have“, wenn es um die Verwaltung einer Angriffsfläche geht.

Endgerät und Verantwortung (Endpoint Device & Responsibility – EDR)

einschließlich Intrusion Detection System (IDS) & Intrusion Prevention System (IPS)

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

EDR-Lösungen können unbefugte Zugriffe erkennen und sogar stoppen, bevor sie passieren. Diese werden oft mit anderen Lösungen für den Erstzugang kombiniert, wie z.B. Firewalls oder Antiviren- und Antimalware-Schutz. Diese Tools können auch auf einer Firewall eingesetzt werden, z.B. zur Erkennung der Herkunft nicht autorisierter IP-Adressen. EDR-Lösungen können automatisiert werden, um Zugriffspatrouillen und Trends im Datenverkehr zu erkennen, die von der Basislinie abweichen, um vor möglichen Angriffen zu warnen.

Wie es hilft, sich zu verteidigen

Sie können nur auf die Vorfälle reagieren, von denen Sie wissen. Je mehr Alarme und Fallen Sie für Hacker aufstellen können, desto mehr Angriffe werden Sie erkennen – und abwehren können.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Warum für EDR bezahlen, wenn wir eine kostenlose Firewall haben?

Erklären Sie einem Nicht-InfoSec-Benutzer, dass dies der Unterschied zwischen einer Mauer und einer Mauer mit Torwächtern ist. Die Mauer ist eine großartige Abschreckung, aber sie scannt nicht proaktiv nach Bedrohungen und versucht, sie am Durchkommen zu hindern.

EDRS kann eine Menge automatischer Sicherheit für eine relativ geringe Investition sein, sowohl in Bezug auf Geld als auch auf Menschen.

Warum dauert es so lange?

Erinnern Sie Ihren Stakeholder daran, dass hinter den Kulissen eine Menge an Feinabstimmung erforderlich ist – Dinge, um die sich Ihr Team kümmert, so dass seine Teams nicht einmal wissen, dass es sie gibt, wenn die Implementierung abgeschlossen ist.

Außerdem muss Ihr Team die Erstinstallation über einen längeren Zeitraum hinweg überwachen, um sicherzustellen, dass den Ergebnissen des EDR vertraut werden kann, was dazu führen kann, dass auch nach der Implementierung noch Optimierungen vorgenommen werden, die zu Problemen führen.

Erkennung und Isolierung bösartiger Verschlüsselungen

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)

Beschreibung

Wenn ein bösartiger Akteur beginnt, Dateien zu verschlüsseln oder zu exfiltrieren oder Lösegeld oder Diebstahl zu fordern, kann diese Art von Software automatisch die angegriffenen Dateien erkennen und Teile des Netzwerks oder Servers isolieren, um eine weitere Verschlüsselung zu verhindern.

Wie es hilft, sich zu verteidigen

Wenn alles andere fehlschlägt, kann die Erkennung und Isolierung bösartiger Verschlüsselungen dazu beitragen, Cyberkriminelle zu entdecken, bevor sie genug Daten stehlen oder sperren, um Schaden anzurichten.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Warum sollten wir dafür bezahlen?

Erinnern Sie Ihren nicht-InfoSec Stakeholder an das Sprichwort: „Erwarte das Beste, aber sei auf das Schlimmste vorbereitet.“

Während Ihre anderen Sicherheitstools Cyberangriffe hoffentlich stoppen, bevor sie diesen Punkt erreichen, kann diese Software als Notbremse fungieren, wenn sie eine Verschlüsselung oder Exfiltration sensibler Daten entdeckt.

Und wie würde die Öffentlichkeit reagieren, wenn sie wüsste, dass Sie nicht jede mögliche, realistische Chance zum Schutz ihrer Daten nutzen? Oder Ihre Aktionäre, um ihre Investitionen vor dem Diebstahl von geistigem Eigentum zu schützen?

Wir haben eine Cyberversicherung, warum sollten wir noch mehr tun?

Eine Cyberversicherung kann Ihnen helfen, die Kosten für die Schadensbegrenzung und die Aufräumarbeiten zu tragen, aber es wird immer noch astronomisch billiger und einfacher sein, sich mit einer Pressemitteilung über einen gestoppten Einbruch zu befassen, als die Aufräumarbeiten nach einem ausgewachsenen Einbruch.

Ihre Versicherungsprämie würde in die Höhe schießen, und Sie müssten wahrscheinlich zusätzliche – und vielleicht sogar teurere – Sicherheitsvorkehrungen treffen, nur um versicherbar zu sein.

Segmentierung des Netzes

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)

Beschreibung

Netzwerksegmentierung ist die Aufteilung der Internet- und Intranet-Netzwerke eines Unternehmens, so dass nur bestimmte Geräte auf bestimmte Teile von Anwendungen oder Servern zugreifen können. Das kann so einfach sein wie Internet-of-Things (IoT)-fähige Geräte in ihrem eigenen Netzwerksegment oder so kompliziert wie jede Abteilung und jeder Server mit ihrer eigenen Umgebung und ihrem eigenen Netzwerk.

Wie es hilft, sich zu verteidigen

Die Netzwerksegmentierung verhindert, dass Hacker auf einen anderen Teil des Netzwerks zugreifen können, auf den sie mit ihren ursprünglich kompromittierten Anmeldeinformationen oder ihrem Zugangspunkt nicht zugreifen konnten. Wenn ein Angreifer in einen harmlosen Teil Ihrer Umgebung eindringt – zum Beispiel in einen IoT-fähigen Toaster – hat er keinen größeren Zugriff auf sensible Daten.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Warum sollten wir so viel für ein Tool zur Netzwerksegmentierung bezahlen?

Tools zur Netzwerksegmentierung können dem Sicherheitsteam Zeit und Ressourcen sparen, indem sie Eindringlinge im Netzwerk identifizieren und den autorisierten Datenfluss zwischen Umgebungen intuitiver gestalten.

Erinnern Sie also Ihre nicht an InfoSec interessierten Stakeholder daran, dass Sie weniger Zeit für die Verwaltung oder Überwachung von Netzwerken aufwenden müssen, um sich den anderen Aufgaben zu widmen, um die sie Ihr Team gebeten hat.

Und je ausgeklügelter Ihr Tool ist, desto weniger Mühe wird es für Ihr Team sein, bei Bedarf von einem Netzwerksegment zum anderen zu wechseln.

Warum ist es dann so schwer, die benötigten Dokumente aus dieser Umgebung zu bekommen?

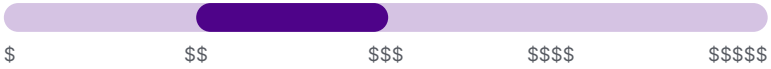
Versuchen Sie, den Prozess für Ihre Stakeholder, die nicht aus dem Bereich InfoSec kommen, so einfach und intuitiv wie möglich zu gestalten.

Erinnern Sie Ihr Team daran, bei Beschwerden so geduldig wie möglich zu sein – besonders zu Beginn! Sie können viele dieser Beschwerden minimieren, indem Sie proaktiv Führungskräfte aus allen Abteilungen als Projektberater in den Implementierungsprozess einbeziehen und Ihnen mitteilen, wer Zugriff auf welche Segmente und deren allgemeine Arbeitsabläufe benötigt.

Passwortlose Multi-Faktor-Authentifizierung (MFA)

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Passwortlose MFA sind Anmeldetools, die für den Zugriff auf Anwendungen oder die Erteilung von Berechtigungen eine sekundäre Authentifizierung erfordern – über Text/SMS, E-Mail, Authentifizierungs-Apps oder sogar biometrische Daten. Im Gegensatz zur traditionellen Zwei-Faktor-MFA ist für die passwortlose MFA-Anmeldung jedoch kein Passwort erforderlich.

Wie es hilft, sich zu verteidigen

Der durchschnittliche Nicht-InfoSec-Mitarbeiter wird es in der Regel vermeiden, komplizierte oder einzigartige Passwörter zu erstellen. Durch die Eliminierung von Passwörtern können Hacker nicht mehr auf Systeme zugreifen, indem sie Anmeldeinformation aus anderen Hacks nutzen, Passwörter mit Brute-Force-Methoden knacken oder ein Mitarbeiter sein Passwort auf einem Klebezettel hinterlässt.

Außerdem können passwortlose MFA-Programme dazu beitragen, die Einhaltung von Sicherheitsprogrammen zu verbessern, da sie sich eine Sache weniger merken müssen!

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Warum kostet die passwortlose MFA so viel mehr als die Alternativen?

Es gibt eine Reihe von passwortlosen MFA-Tools. Im Allgemeinen gilt: Je höher die Kosten pro Benutzer, desto höher die verfügbaren Verschlüsselungsstufen und benutzerdefinierten Kontrollen.

Eine bessere Verschlüsselung verhindert, dass Hacker das System mit schierer Computerleistung knacken können.

Außerdem können benutzerdefinierte Steuerelemente dazu beitragen, die Arbeitskosten zu senken und gleichzeitig die Benutzerfreundlichkeit für alle zu erhöhen.

Die Time-Out-Sessions sind so lästig! Können Sie das verhindern?

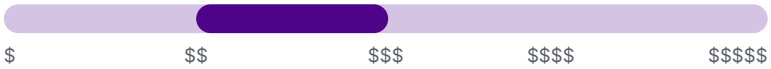
Erstens können Sie je nach Beziehung zum Stakeholder scherzen und sagen: „Wenn Sie schon denken, dass die nervig sind, stellen Sie sich vor, wie viel frustrierender es für einen Hacker ist, ständig rausgeschmissen zu werden! Sie kommen wenigstens wieder rein.“

Etwas ernsthafter können Sie dem Stakeholder, der nicht aus dem Bereich InfoSec kommt, dann zeigen, dass der Zugriff auf das Netzwerk nur der erste Teil eines Cyberangriffs ist, und zwar mit einigen der Verteidigungspläne, die Sie weiter unten in diesem eBook finden. Je schwieriger das Unternehmen es unbefugten Hackern macht, im System zu bleiben, desto einfacher wird es für Ihre Teams sein, die Invasion zu beenden und sie endgültig zu vertreiben.

Verwaltung von Privilegien

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Die Rechteverwaltung steuert, welche Arten von Mitarbeitern welche Berechtigungen auf ihren persönlichen oder Netzwerkrechnern benötigen. Der durchschnittliche Büroangestellte könnte beispielsweise den Power-Admin-Status auf seinen persönlichen Computern verwenden, benötigt aber im Allgemeinen keine Berechtigungen für die Installation der PowerShell.

Wie es hilft, sich zu verteidigen

Ähnlich wie bei der Zugriffskontrolle: Wenn ein Hacker auf den Desktop-Computer eines durchschnittlichen Mitarbeiters zugreifen würde – für den dieser Mitarbeiter als Superadministrator angemeldet war –, könnte er aufgrund der begrenzten Berechtigungen immer noch nicht viele Hacking-Tools einsetzen und sich größeren Zugang zum Netzwerk verschaffen.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Warum sollten wir dafür auch noch bezahlen?
Es wird mehr Personal für die Bereitstellung und Verwaltung benötigt!

Ja, in der Regel ist die Implementierung und Pflege von Programmen zur Verwaltung von Berechtigungen mit einem höheren Arbeitsaufwand verbunden, da sie ständig überwacht und auf Benutzerebene aktualisiert werden müssen. Dieser erhöhte Wartungsbedarf ist der Grund, warum es im Allgemeinen von Unternehmen oder Organisationen in stark regulierten Branchen verwendet wird.

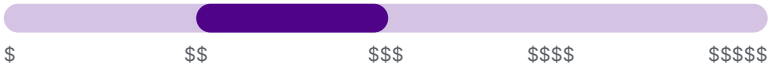
Wenn also die Kosten oder die interne Unterstützung für dieses Programm bei anderen Stakeholdern, die nicht aus dem Bereich InfoSec kommen, ein Problem darstellen, dann sollten Sie die Diskussion für dieses Jahr zurückstellen. Achten Sie dann beim Onboarding genauer auf die anfänglichen Berechtigungen und vermeiden Sie es in der Regel, jemandem Admin-Zugriffsrechte zu gewähren.

Wenn Sie mehr (qualifizierte) Anfragen für Ausnahmen von Ihren Regeln erhalten, sammeln Sie diese Anfragen als Argumente für eine technischere Lösung für das Privilegienmanagement. Irgendwann wird es wirtschaftlich sinnvoll sein, in ein Tool zu investieren, das zumindest einen Teil des Prozesses für Sie automatisieren kann.

Risikobasiertes Patch- und Schwachstellenmanagement

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Die Tools identifizieren und priorisieren Korrekturen auf der Grundlage der Umgebung und der Bedürfnisse eines Unternehmens – und rollen diese Patches auch aus! – anstelle von Patches, die auf externen Sicherheitslücken beruhen, die von kritischen Stellen oder Anbietern bewertet werden.

Wie es hilft, sich zu verteidigen

RBPM- und RBVM-Tools helfen Unternehmen dabei, die Patches und Sicherheitslücken zu priorisieren, die für ihre Geräte und Anwendungsfälle am wichtigsten sind. Dazu gehört auch die Hervorhebung der Schwachstellen und Sicherheitslücken, die Cyberkriminelle gerade jetzt nutzen!

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Haben wir vorher nicht gepatcht? Was ist der Unterschied?

Bestätigen Sie zunächst, dass Ihr Team schon vorher gepatcht hat, aber erinnern Sie Ihren Stakeholder an die Feueralarmübungen, die immer wieder stattfinden. Würden Sie die Notfälle aufgrund von Schlagzeilen nicht gerne vermeiden? RBVM und RBVM können proaktiv die wichtigen Punkte identifizieren und patchen, bevor die Hacker zu Ihnen kommen.

Dann verweisen Sie ausdrücklich auf die Defense Plays der Bedrohungsakteure, die im Jahr 2022 Organisationen wie die Ihre angegriffen haben, um Punkt für Punkt zu zeigen, wo das Patchen ausgenutzter oder älterer Schwachstellen Angriffe frühzeitig gestoppt hätte.

Betonen Sie abschließend, dass Sie diese Art von Patching nicht manuell durchführen können. Nur RBPM und RBVM können automatisch herausfinden, welche Exploits für Ihre einzigartige Bedrohungsumgebung von Bedeutung sind – und bestimmen, ob Ihre Geräte und Daten geschützt sind!

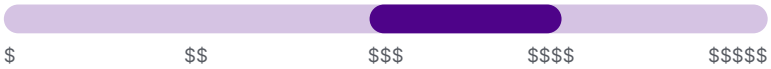
Warum sollten wir für dieses Tool bezahlen, wenn es kostenlose Auto-Patch-Software-Versionen gibt?

Weisen Sie darauf hin, dass risikobasierte Tools zur Verwaltung von Sicherheitslücken mehrere Kontaktpunkte für Angreifer beeinflussen können. Daher können Investitionen in RBVM- und RBPM-Tools – eines zur Priorisierung und das andere zum Ausrollen von Patches – mehrere Angriffspunkte während eines Hacks verhindern, selbst wenn Sie nicht wissen, dass sich ein Hacker im System befindet.

Sicherheitsprogramm-Audits

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Sicherheitsprogramm-Audits umfassen eine breite Palette von Dienstleistungen, werden aber im Allgemeinen als externe Berater oder Analysten zusammengefasst, die sicherstellen, dass Cybersicherheitslösungen und -programme funktionieren, dass Umgebungen und Rollen noch in Ordnung sind und dass Anpassungen erforderlich sind. Penetrationstests und Phishing-Schulungen für Mitarbeiter können in diese Kategorie fallen.

Wie es hilft, sich zu verteidigen

Offen gesagt ist es für jemanden, der in ein Programm oder Projekt involviert ist, sehr schwierig, dessen Schwächen zu erkennen. In vielen Fällen ist ein externes Sicherheitsaudit durch einen vertrauenswürdigen Anbieter die einzige Möglichkeit zu erfahren, ob Ihr Sicherheitsprogramm tatsächlich so funktioniert, wie Sie es geplant haben.

Tiefgreifende Audits können auch Merkwürdigkeiten oder schlummernde Eindringlinge aufspüren, die entweder von internen Bedrohungen oder externen Hackern stammen. Ein Audit kann auch lose Enden und zufällige Details bereinigen, die nicht mit ihren aktuellen Rollen abgeglichen oder neu ausgerichtet wurden.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Haben wir nicht gerade ein Audit durchgeführt? Warum für ein weiteres bezahlen?

Audits sollten häufiger bei risikoreichen Umgebungen, Partnern und Anbietern durchgeführt werden. Je mehr eine Umgebung mit geschäftskritischen Systemen oder mit bekannten Zielen oder Angreifern verbunden ist – wie z.B. einer Regierungsbehörde oder einem militärischen Auftragnehmer – desto wahrscheinlicher ist es, dass ein Hacker versucht, auf die Umgebung zuzugreifen.

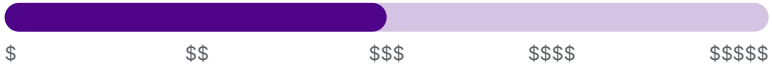
Häufige Audits können auch einen lauernden Hacker erwischen, der Informationen sammelt, bevor der Angriff richtig gestartet wird. Die frühzeitige Identifizierung besonders versierter Angreifer kann Ihrem Unternehmen Millionen an Datenverlusten, Reputationsverlusten und Rechtskosten ersparen.

Strategische Automatisierung

Warnungen und Erlaubnisanfragen

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

In diesem Zusammenhang geht es um automatische Benachrichtigungen über unerwünschte oder unerwartete Aktivitäten wie z. B. seltsame oder unpassende Genehmigungsanfragen. Automatisierung kann auch dazu beitragen, die täglichen Aktivitäten für allgemeine Sicherheitsprogramme zu erleichtern.

Wie es hilft, sich zu verteidigen

Ein einziges Ereignisprotokoll könnte selbst von den detailorientiertesten Sicherheitsexperten unbemerkt bleiben. Dasselbe Ereignis könnte jedoch eine Warnschwelle auslösen, um das richtige Abhilfeteam zu informieren und automatisch einen nahtlosen Prozess der Analyse und Abhilfe einzuleiten.

Da die Bedrohungen immer komplexer werden und die Zuständigkeiten des InfoSec-Teams wachsen, kann die Automatisierung den überforderten und nicht einstellbaren Sicherheitsteams helfen, ihre Aufgaben zu erfüllen, ohne dass die Sicherheit des Unternehmens darunter leidet.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Warum für Automatisierungstools bezahlen?

Oft ist es billiger und genauer, für mehr automatisierte Lösungen zu bezahlen, als mehr Sicherheitsexperten einzustellen ... wenn Sie überhaupt einen qualifizierten Kandidaten für die Stelle finden können.

Häufig ist die Automation eine der wichtigsten Eigenschaften anderer Tools. Es kann ein zusätzlicher Nutzen sein, der die Wahl eines Tools oder einer Lösung gegenüber einer anderen rechtfertigt.

Wir haben die Automatisierung schon einmal ausprobiert, und sie hat alles kaputt gemacht.

Weisen Sie nervöse Stakeholder darauf hin, dass Automatisierung kein Ersatz für eine menschliche Beurteilung ist und nicht unüberlegt, ungetestet und ohne Rücksicht auf die Störung von Geschäftsabläufen eingeführt wird.

Listen Sie daher bei Ihrer Anfrage genau auf, was Ihre Automatisierung tun wird und was nicht, um die Erwartungen festzulegen und die Nerven zu beruhigen.

Warum müssen wir immer noch Tickets für Zugriffsanfragen einreichen? („Können wir <Service X> automatisieren?“)

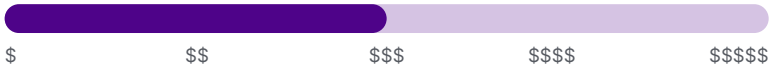
Die Automatisierung kann zwar einen Teil des Verwaltungsaufwands abnehmen, aber Hacker können und werden sich vollständig automatisierte Systeme zunutze machen.

So könnten Hacker beispielsweise einen vollständig automatisierten Zugriffsanforderungsprozess austricksen, um höhere Berechtigungen zu erhalten und mehr Bereiche des Netzwerks zu erreichen. Eine menschliche Kontrolle kann diese Eskalation auffangen und stoppen.

Benutzerzugriffskontrolle

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Tools zur Kontrolle des Benutzerzugriffs helfen dabei, proaktiv zu verwalten, welche Mitarbeiter und deren Funktionen für ihre Aufgaben Zugriff auf welche Teile des Netzwerks und Anwendungen benötigen. Diese Tools helfen auch dabei, den Zugriff auf frühere Berechtigungen zurückzuziehen, da sich Aufgaben und Rollen im Laufe der Zeit ändern.

Wie es hilft, sich zu verteidigen

Selbst wenn ein Hacker die Zugangsdaten eines durchschnittlichen Mitarbeiters erlangt hat, erlaubt die Benutzerzugriffskontrolle dem Hacker nur den Zugriff auf das, was dieser Mitarbeiter konnte – nicht auf alle möglichen Dateien oder Datenserver. Die Zugriffskontrollen können auch bei ungewöhnlichen Zugriffsanfragen oder Einbruchsversuchen Alarm schlagen und so frühzeitig auf Seitenbewegungen von bisher unentdeckten Hackern aufmerksam machen.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Warum kostet die Zugriffskontrolle für Benutzer so viel?

Im Allgemeinen handelt es sich bei den Tools zur Benutzerzugriffskontrolle um ein „Pay-per-Seat"-Modell. Je größer Ihr Unternehmen also wird, desto mehr wird es insgesamt kosten – und Sie müssen auch jedes Jahr Änderungen an der Budgetzuweisung planen, je nachdem, wie Ihr Unternehmen wachsen oder sich konsolidieren will.

Versuchen Sie, die Frage in Bezug auf eine Versicherung pro Person zu formulieren. Wäre der Stakeholder bereit sein, x € pro Person zu zahlen, um das Risiko zu vermeiden, dass ein durchschnittlicher Mitarbeiter versehentlich seine Zugangsdaten auf dem Laptop liegen lässt und damit Ihr gesamtes geistiges Eigentum und Ihre Kundendaten preisgibt - selbst wenn er Zugang zu diesen Informationen benötigen?

Ich habe keinen Zugang mehr zu dem, was ich brauche!

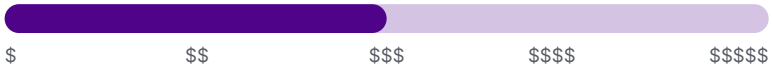
Versuchen Sie, das Verfahren zur Einreichung von Anträgen auf Änderungsgenehmigungen für Ihre Nicht-InfoSec-Stakehoolder so einfach und intuitiv wie möglich zu gestalten.

Erinnern Sie Ihr Team daran, bei Beschwerden so geduldig wie möglich zu sein – vor allem am Anfang! Sie können viele dieser Beschwerden minimieren, indem Sie proaktiv Führungskräfte aus allen Abteilungen als Projektberater in den Implementierungsprozess einbeziehen und Ihnen mitteilen, wer Zugriff auf welche Anwendungen und deren allgemeine Arbeitsabläufe benötigt.

Benutzerschulung und Ausbildung

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Sicherheitstraining und -ausbildung für den durchschnittlichen Nicht-InfoSec-Mitarbeiter kann von grundlegenden Trainingsmodulen bis hin zu aufwendigen Tabletop-Übungen und immersiven Simulationen reichen.

Wie es hilft, sich zu verteidigen

Der Mensch ist das schwächste Glied in jeder Sicherheitskette. Jede noch so gute Technologie der Welt kann nicht immer Sicherheitsunfälle verhindern, die die von den wohlmeinendsten Personen ausgelöst werden. Schulungen helfen, die Mitarbeiter zu befähigen, Verantwortung für ihre eigene Cybersicherheit zu übernehmen, ihr eigenes Verständnis zu stärken und die Sicherheitsumgebung des gesamten Unternehmens.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Wie können wir Schulungen effektiv durchführen?

Schaffen Sie Anreize für Nicht-InfoSec-Mitarbeiter, ihre Ausbildung zu nutzen, indem Sie Mitarbeiter über Angriffe informieren, die sie persönlich verhindert haben, z. B., wenn sie einen Phishing-Angriff melden.

Sie können auch dazu beitragen, gesunde Sicherheitsprotokolle durchzusetzen, indem Sie Passwortmanager subventionieren.

Versuchen Sie in der Regel nicht, Mitarbeiter für die Nichteinhaltung von Vorschriften zu bestrafen. Hervorheben und loben Sie stattdessen bewusst regelkonformes Verhalten, um Sicherheit zu einer gemeinsamen Verantwortung zu machen.

Warum kostet die Schulung zur Benutzersicherheit so viel?

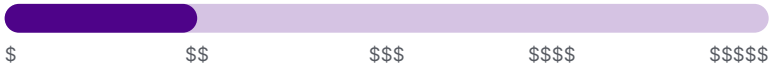
Effektive Benutzerschulungen sind in der Regel interaktiv und hochwertig produziert – manchmal sogar mit eigenen Skripten! Diese Schulungsmodule sind schwer zu erstellen und können daher recht teuer sein.

Doch je interaktiver und relevanter ein Benutzer, die Schulung empfindet, desto größer ist die Beteiligung und desto besser bleibt das Wissen erhalten – was bedeutet, dass er sein Sicherheitswissen nutzen kann, wenn es am wichtigsten ist.

Webbasierte Inhaltsbeschränkungen

Zeit bis zur Funktionalität

Kosten für kostenpflichtige Tools (Einstieg in robuste Lösungen)



Beschreibung

Diese Tools schränken ein, was Benutzer online sehen oder aufrufen können, während sie von einem geschützten Gerät aus arbeiten.

Wie es hilft, sich zu verteidigen

Angreifer und andere Hacker können Daten und Material über Online-Anwendungen weiterleiten. Wenn Sie den Zugang zum Internet einschränken, schränken Sie auch andere Bedrohungen ein - einschließlich möglicher Malware und Eindringlinge von außen, die sich sonst im Internetverkehr „verstecken“ könnten.

Wappnen Sie Ihre Mitarbeiter! - Rechtfertigung gegenüber Stakeholdern

Warum sollte man ein Tool kaufen, das Webinhalte einschränkt?

Normalerweise wird diese Art von Tool in stark reglementierten On-Site-Umgebungen implementiert. Grund dafür sind die Komplexität der Implementierung – die Abwägung zwischen Beschränkungen von ablenkenden oder gefährlichen potenziellen Online-Inhalten und den tatsächlichen, arbeitsbezogenen Online-Anforderungen – und die wachsende Beliebtheit von Remote-Arbeit.

Zu diesen Organisationen gehören oft Regierungseinrichtungen, Krankenhäuser, Callcenter und sogar Banken mit ihren Geldautomaten.

Wenn Ihr Unternehmen jedoch in stark regulierte Bereiche wie das Finanzwesen, das Gesundheitswesen oder die Regierung vordringen möchte, können sich restriktivere Tools für Sie lohnen.

Sie könnten auch einen Produktivitätsschub erleben – aber seien Sie vorsichtig, wie Sie diesen Vorteil anpreisen. Die Produktivität wird nur dann verbessert, wenn die Mitarbeiter weiterhin auf die Inhalte und Ressourcen zugreifen können, die sie für ihre Arbeit benötigen, und wenn ablenkende Websites während der Arbeitszeiten gesperrt werden.

Ausgewählte Angreifer 2022

Obwohl es im Jahr 2022 eine ganze Reihe von Cybersecurity-Vorfällen gab, die von einer Vielzahl von kriminellen Gruppen und Motivationen verursacht wurden, haben wir vier ganz unterschiedliche Bedrohungen ausgewählt, die wir hier vorstellen.

Jede dieser Gruppen bietet zahlreiche relevante Beispiele, die Ihnen dabei helfen werden, Ihre strategischen Cybersecurity-Ziele für 2023 voranzutreiben – ganz gleich, was Sie erreichen wollen.

ivanti CSW Cyber SecurityWorks

Ausgewählte Angreifer 2022

In diesem Abschnitt

ALPHV

Die ALPHV-Gruppe - auch bekannt als „BlackCat“ und als die jüngste öffentliche Iteration der Hacker-Gangs BlackMatter und DarkSide – ist ein Paradebeispiel für eine cyberkriminelle Bande, die für die Entwicklung, den Verkauf und die Bereitstellung eines „Ransomware-as-a-Service“-Modells (RaaS) verantwortlich ist.

Was ist RaaS? Und warum sollten sich Ihre Stakeholder dafür interessieren?

RaaS ist im Grunde eine Organisation, die zum Teil vom Verkauf von Hacking-Softwarepaketen im Dark Web oder über verschiedene Broker profitiert.

Mit ein wenig strategischem Social Engineering, um über kompromittierte Anmeldeinformationen in das Computersystem oder Netzwerk eines Ziels einzudringen, sperrt RaaS alle wichtigen Dateien, es sei denn, das Opfer erklärt sich bereit, ein Lösegeld im Austausch für einen digitalen Schlüssel zu zahlen.

Als Ersteller der Originalsoftware verlangt ALPHV einen Prozentsatz der eingenommenen Lösegeldgebühren, ohne dass eine zusätzliche Schmutzarbeit anfällt. (Abgesehen davon kann die Bande ausgewählte Ziele direkt angreifen und kassiert dabei 100 % des Lösegelds.)

RaaS unterscheidet sich in zweierlei Hinsicht von gewöhnlicher Ransomware:

1. Indem sie die Ransomware-Software verpacken und verkaufen, schreiben ALPHV und andere RaaS-Anbieter Code im Auftrag anderer Krimineller, die nicht selbst programmieren können (oder wollen) – was das Risiko potenzieller Cyberangriffe insgesamt exponentiell erhöht.

   Und wenn Hacker nicht wissen müssen, wie sie ihren eigenen Code schreiben müssen, um jemanden zu hacken, dann wird jeder mit schlechten Absichten zu einer Cyberbedrohung.

2. Nationale Angreifer wie Nobelium verwenden Hacks „von der Stange“ wie BlackCats RaaS als Teil ihrer Spionage oder Angriffe auf ausländische Mächte. Sie beschleunigen Angriffe und verschleiern ihre Beteiligung, indem sie den Code anderer verwenden, während sie ihre eigenen geheimen Hacks für wertvollere Ziele behalten.

Während die Einführung und Ausweitung von RaaS als „Geschäftsmodell” im Dark Web weiterhin zu einem unglaublichen Anstieg der Angriffe auf alle möglichen Organisationen, Unternehmen und Behörden führt, stellt dies auch eine Chance für versierte Sicherheitsteams dar.

Warum? Denn wenn viele Hacker dieselben oder ähnliche Exploits „von der Stange” verwenden, indem sie dieselbe oder ähnliche Ransomware einsetzen, dann können schon wenige Präventivmaßnahmen eine große Zahl von Angriffen verhindern.

ALPHV Datenblatt

Aliases:

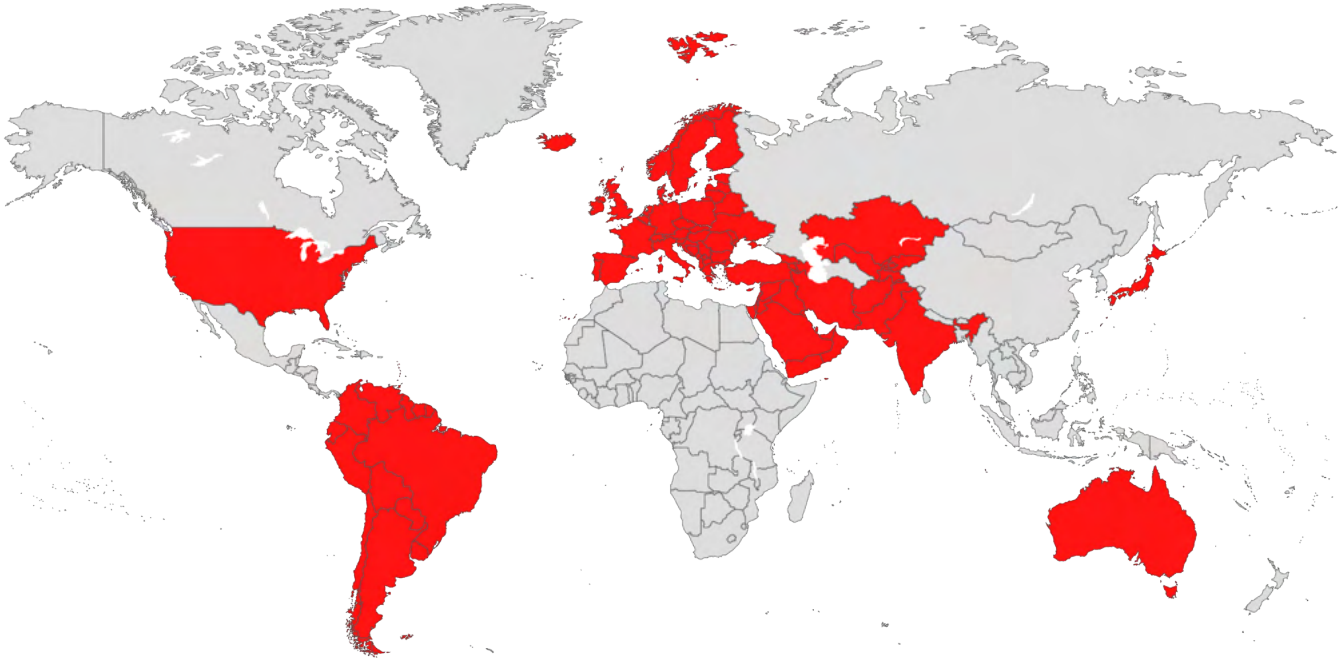
BlackCat
ALPHV
ALPHA
Noburus
AlphaVM

Motive:

Kriminell / Finanziell

Bedrohungstyp:

Ransomware-as-a-Service-Bande



Zugehörigkeit und Verbindungen

Russland
Ryuk
Revil
DEV-0504
DEV-0237
FIN12
FIN7
Conti
BlackMatter
DarkSide

Bevorzugte Exploits:

CVE-2016-0099
CVE-2019-7481
CVE-2021-31207
CVE-2021-34473
CVE-2021-34523

Bekannte Zielregionen:

Australien
Österreich
Europa
Deutschland
Indien
Italien
Japan
Naher Osten
Südamerika
Schweiz
USA

Auswirkungen ausgewählter ALPHV-Angriffe auf das Unternehmen

> Der vorübergehende Ausfall der IT-Dienste [...] hatte Auswirkungen auf den Betrieb des Logistikzentrums und die Kundenbetreuung.

23. Dezember 2021:
Moncler | Mode / Einzelhandel | Mailand

> „Die Terminals arbeiten mit begrenzter Kapazität und haben höhere Gewalt [ein äußeres, unabwendbares und unvorhersehbares Ereignis] erklärt.
>
> „Betroffen sind 233 Tankstellen in Norddeutschland. Es ist wahrscheinlich möglich, in bar zu bezahlen."

29. Januar 2022: Oiltanking + Mabanaft | Logistik | Deutschland

> „Die IT-Mitarbeiter dort arbeiten buchstäblich rund um die Uhr, um diesen Angriff zu beheben. Ich fühle wirklich mit den Kollegen dort, die gerade eine Herkulesarbeit leisten, um uns wieder voll funktionsfähig zu machen."

7. bis 11. März 2022: North Carolina A&T State University | Bildung | USA

> "„Wir gehen davon aus, dass von den 3.000 betroffenen IT-Arbeitsplätzen die ersten [vier Tage nach dem Angriff] wieder zur Verfügung stehen werden. [...] Da man von den IT-Systemen abhängig ist, befindet sich die Verwaltung im Notfallmodus."

14. Mai 2022: Kärnten | Regierung | Österreich

> „Auf die Frage, ob die Daten von [ALPHV] verschlüsselt oder kopiert wurden, sagte ein Sprecher, dass die Firma nicht über diese Aussage hinausgehen wird."

31. Mai 2022: CMC ELectronics | Elektronik | Militär / Raumfahrt | Kanada

> „Es besteht die Möglichkeit, dass Kundendaten [...] auf den [angegriffenen] Servern und PCs enthalten waren, und wir ermitteln derzeit [...] das Vorhandensein eines Lecks, den Umfang des Schadens und untersuchen die Ursache."

3. Juli 2022: Bandal Namco | Unterhaltung | Japan

> „Da unsere Systeme seit Tagen nicht mehr zugänglich sind, arbeiten wir hart daran, den entstandenen Rückstand aufzuholen."

22.-23. Juli 2022: Creos | Energie | Luxemburg

> „Wir gehen davon aus, dass die Gebäude am Montag weiterhin geschlossen bleiben, ohne dass es einen genauen Zeitplan für die Wiedereröffnung gibt. [...]
>
> Wir haben verstanden, dass wir verwundbar sind."

17. August 2022: Fremont County | Regierung | USA

Eine ALPHV Cyberdefense Strategie:
Wie Sie ALPHV-Angriffe vor einer Lösegeldforderung stoppen können

Zugang zum Netzwerk über kompromittierte Zugangsdaten.

Hacker zu stoppen, bevor sie in das Netzwerk eindringen, ist der einfachste, billigste und schnellste Weg, jede Geschäftseinheit zu schützen, ohne den Betrieb zu unterbrechen.

- EDR
- Webbasierte Inhaltsbeschränkungen
- Antivirus / Antimalware
- Anti-Phishing für Mobiltelefone
- Benutzerschulung und Ausbildung
- Passwortlose MFA
- Benutzerzugriffskontrolle
- Anwendungskontrolle
- Gerätehygiene und -management
- Sicherheitsprogramm-Audits
- Strategische Automatisierung
- Konfigurationsmanagement

Kartierung Systeminformationen und Netzwerk

Wenn sich Eindringlinge nicht frei oder leicht im Netzwerk bewegen können, können sie keine wichtigen Daten oder Sicherheitslücken finden – wasdie Auswirkungen auf das Geschäft verringert.

- Risikobasiertes Patch- und Schwachstellenmanagement
- Geräte- und Netzwerksegmentierung
- Gerätehygiene und -management
- Asset-Abstimmung
- Sichere Zugangsprotokolle
- Segmentierung des Netzes
- Verwaltung von Privilegien
- Strategische Automatisierung
- Konfigurationsmanagement

Erstellen von opferspezifischer Ransomware basierend auf einzigartigen „Löchern“ oder Exploits.

Wenn Cyberkriminelle ihre Ransomware nicht starten können, können sie auch keine Daten für Lösegeld sperren oder stehlen.

- Risikobasiertes Patch- und Schwachstellenmanagement
- Anwendungskontrolle
- Benutzerzugriffskontrolle
- Verwaltung von Privilegien
- Gerätehygiene und -management
- Strategische Automatisierung

Sicherheitsprogramme daran hindern, den Ransomware-Angriff oder die Löschung von Daten zu blockieren.

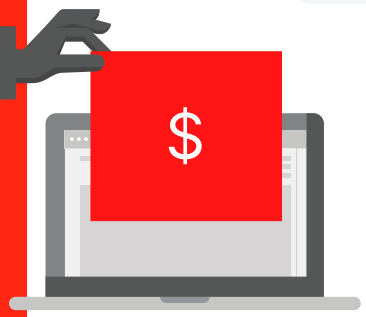
Ungewöhnliche Verhaltenswarnungen können das Anfangsstadium eines Ransomware-Angriffs signalisieren, bevor der Betrieb eingestellt wird oder Lösegeld gefordert wird.

- Anwendungskontrolle
- Strategische Automatisierung
- Benutzerzugriffskontrolle

Verschlüsselung von Dateien und Datenexfiltration (Entfernen oder Kopieren aus dem System), um ein Druckmittel gegen das Opfer zu schaffen.

Wenn die Hacker keine Daten stehlen oder sperren können, haben sie kaum ein Druckmittel, um ein Lösegeld zu fordern.

- Erkennung und Isolierung bösartiger Verschlüsselungen
- Geräte- und Netzwerksegmentierung
- Webbasierte Inhaltsbeschränkungen



Für proaktive Prävention ist es zu spät; wechseln Sie in den „Disaster Recovery“-Modus.

APT29

Die berüchtigten Hacker, die die internen E-Mails und Dokumente des Demokratischen Nationalkomitees durchsickern ließen, APT29, oder „Nobelium“, ist eine Cyber-Organisation, die mit dem russischen Auslandsgeheimdienst verbunden ist und sich der Spionage und nachrichtendienstlichen Aktivitäten widmet.

„APT“ steht für „Advanced Persistent Threat“. Diese Bezeichnung beschreibt in der Regel eine national oder staatlich gesponserte Bedrohungsgruppe, die in das Netzwerk eines Unternehmens eindringen und sich dort monatelang – sogar jahrelang – aufhalten kann, bevor sie entdeckt oder angegriffen wird.

Warum sollten sich Ihre Stakeholder für den APT29 interessieren, wenn Sie keine Regierungsbehörde sind?

Sobald Stakeholder, die nicht aus dem Bereich InfoSec kommen, hören, dass der Angreifer von Latets, der diese Woche für Schlagzeilen sorgte, dem russischen Geheimdienst angehört, möchten sie die Bedrohung vielleicht ganz abtun.

„Warum sollte sich APT29 für uns interessieren?“, könnten sie sagen. „Wir sind keine Regierungsbehörde! Wir sind nicht Teil der Kriegsbemühungen!“

Hier kommt das Small-World-Problem ins Spiel.

Viele Studien zur Erforschung sozialer Netzwerke – von Dissertationen über Metas Facebook-Forschung bis hin zu Meme-Spielen mit dem Schauspieler Kevin Bacon – haben die Verbindungen zwischen einer Beziehung zur nächsten in Populationen unterschiedlicher Größe untersucht. Die durchschnittliche „Entfernung“ von einem beliebigen Startpunkt zum endgültigen „Ziel“ scheint etwa drei bis vier Verbindungen zu betragen.

Lassen Sie uns dieses hypothetische Szenario nun auf Ihren Vorstoß für eine proaktive Cybersicherheitsstrategie ausweiten.

Auch wenn es sich bei IhremUnternehmennicht um eine Regierungsbehörde oder eine aktivistische Non-Profit-Organisation handelt, die Russland in die Zange nimmt, ist es nicht ungewöhnlich, dass Angreifer Verbindungen zu ihren Endzielen – oder Verbindungen von Verbindungen von Verbindungen über Angriffe auf die Lieferkette – ins Visier nehmen, um Krisen zu beeinflussen und Informationen zu gewinnen.

Nehmen Sie zum Beispiel den berühmten SolarWinds-Vorfall – eine APT29-Cyberattacke aus dem Jahr 2020.

Die APT29-Hacker hatten es nicht direkt auf Regierungsbehörden oder kritische Infrastrukturorganisationen abgesehen. Stattdessen infizierten sie den Softwareanbieter eines Vertragspartners, eine Plattform für Netzwerküberwachungssoftware, um dann über ein routinemäßiges Software-Update Hintertüren bei etwa 18.000 Kunden zu installieren ... darunter auch Nutzer die für die Regierung arbeiteten.

Nicht alle 18.000 Kunden waren das Ziel von APT29, aber alle wurden gehackt – und alle wurden zu Sicherheitslücken, wenn sie in einen Underground-Cyberkrieg zwischen mächtigen Nationen verwickelt werden.

Wenn also einer Ihrer Stakeholder, die nicht aus dem Bereich InfoSec kommen, sich gegen die Vorbereitung auf APT29 oder eine andere hochentwickelte, hartnäckige Bedrohung wehren möchte, weil Sie „neutral“ oder ein Nicht-Kombattant sind, dann spielen Sie das Spiel 6 Degrees of Separation als Tischübung oder als Workshop-Aktivität.

Aber dieses Mal spielen Sie die Verbindungen Ihrer Organisation zu Russland durch.

> **Statistisch gesehen ist Ihr Unternehmen viel näher daran, ein APT29-Ziel – oder ein Ziel für eine andere APT-Gruppe – zu sein, als Nicht-Infosec Stakeholder glauben möchten.**

APT29 Statistikblatt

Aliases:

Nobelium	Cozy Bear	UNC-1151
YTTRIUM	CozyDuke	Cloaked Ursa
The Dukes	UAC-0113	

Motiv:

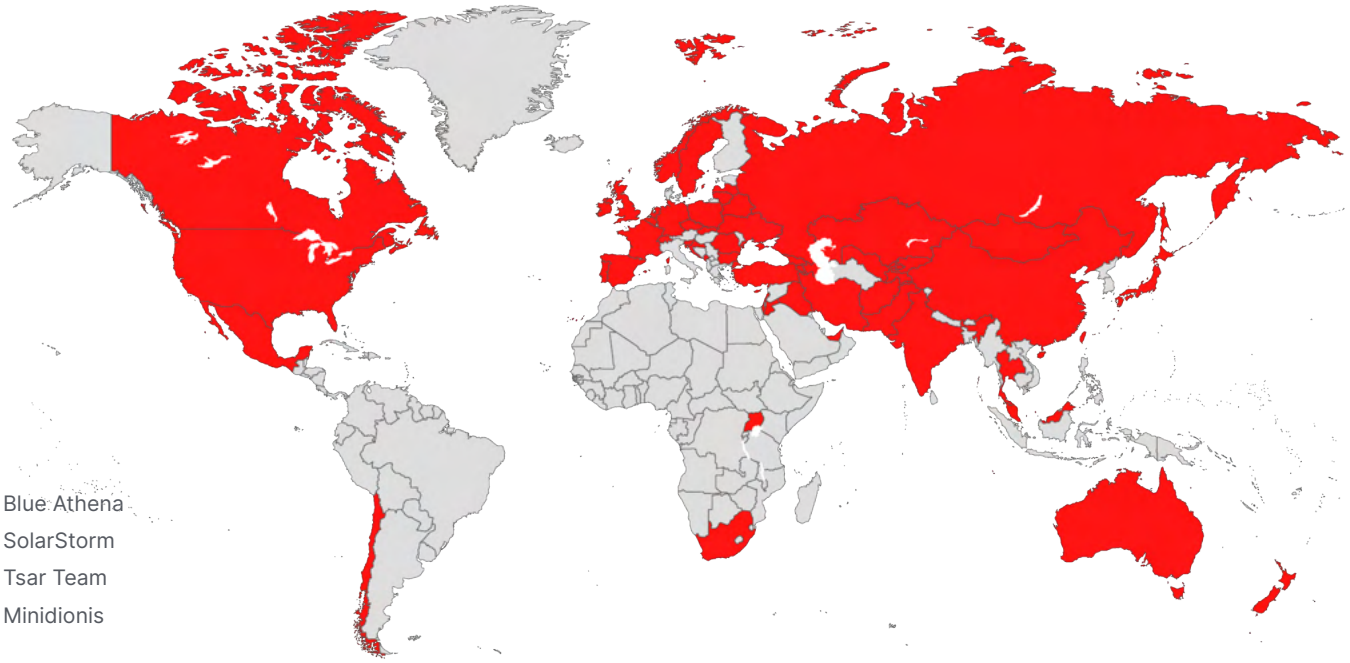
Spionage / Verdeckte Operationen

Threat Type:

Advanced Persistent Threat / APT

Zugehörigkeit und Verbindungen:

Russland	APT28	Actinium	Blue Athena
Conti	Strontium	Bromine	SolarStorm
ALPHV	Iridium	Krypton	Tsar Team
Fighting Ursa	DEV-0586	StellarParticle	Minidionis



Bevorzugte Exploits:

CVE-2009-3129	CVE-2019-17026	CVE-2020-14882
CVE-2014-1761	CVE-2019-19781	CVE-2020-4006
CVE-2015-164	CVE-2019-2725	CVE-2020-5902
CVE-2018-13379	CVE-2019-7609	CVE-2021-1879
CVE-2019-11510	CVE-2019-9670	CVE-2021-21972
CVE-2019-1653	CVE-2020-0674	CVE-2021-26855

Kritische Risikobranchen:

Regierung	NGOs und gemeinnützige Organisationen	Hochschulbildung
Militär		Finanzen
Energie	Transport	Forschung / Think Tanks
Medien und Telekommunikation	IT	
	Gesundheitswesen	

Bekannte Zielregionen:

Afghanistan	Chile	Iran	Litauen	Polen	Schweiz
Armenien	China	Irak	Luxemburg	Portugal	Tadschikistan
Australien	Kroatien	Irland	Malaysia	Rumänien	Thailand
Aserbaidschan	Zypern	Israel	Mexiko	Russland	Türkei
Weißrussland	Tschechisch	Japan	Mongolei	Slowakei	VAE
Belgien	Frankreich	Jordanien	Montenegro	Slowenien	Uganda
Brasilien	Georgien	Kasachstan	Niederlande	Südafrika	Großbritannien
Bulgarien	Deutschland	Kirgisistan	Neuseeland	Südkorea	Ukraine
Kanada	Ungarn	Lettland	Norwegen	Spanien	Vereinigte Staaten
Tschetschenien	Indien	Libanon	Pakistan	Schweden	Usbekistan

Auswirkungen ausgewählter APT29-Attacken auf Unternehmen

Die von APT29 verschickten Phishing-E-Mails gaben sich als Verwaltungsmitteilungen verschiedener Botschaften aus und nutzten legitime, aber kooptierte E-Mail-Adressen.

Der Angriff begann am 17. Januar 2022 – Angekündigt am 28. April 2022: Diplomatische Einrichtungen | Europa, Asien, Nordamerika

„Diese Akteure [einschließlich APT29] nutzen einfache Passwörter, ungepatchte Systeme und ahnungslose Mitarbeiter aus, um sich zunächst Zugang zu verschaffen, bevor sie sich seitlich durch das Netzwerk bewegen, um Persistenz herzustellen und Daten zu exfiltrieren."

Angriff begann im Januar 2020 - Angekündigt am 16. Februar 2022: Zugelassenes Verteidigungsunternehmen | Militär | USA

„Die Administratoren fanden PCs vor, die gesperrt waren und eine Nachricht anzeigten, in der 10.000 Dollar in Bitcoin gefordert wurden, aber die Festplatten der Rechner waren irreversibel beschädigt, als ein Administrator sie neu startete."

13. Januar 2022: Regierung, gemeinnützige & IT-Unternehmen | Ukraine

„Seit Anfang Mai hat Cloaked Ursa [APT29] seine Fähigkeiten weiterentwickelt, Malware über beliebte Online-Speicherdienste zu verbreiten, darunter Dropbox und Google Drive."

Angriff begann im Mai 2022 – Angekündigt am 5. Juli 2022: Ausländische Botschaften | Portugal und Brasilien

Bereits im Mai 2021 nutzten russische Cyber-Akteure ein falsch konfiguriertes Konto bei einer Nichtregierungsorganisation (NGO), das auf die Standard-MFA-Protokolle eingestellt war, um ein neues Gerät für MFA zu registrieren und auf das Netzwerk des Opfers zuzugreifen.

Angriff begann im Mai 2021 – Angekündigt am 15. März 2022: Nichtregierungsorganisation | USA

„Es gibt ein erhöhtes Potenzial für Cyberangriffe. Diese können schwerwiegende Auswirkungen haben, auch für Länder und Organisationen, die nicht direkt [von russischen Cyber-Kampagnen] betroffen sind."

18. Februar 2022: „National bedeutsame Unternehmen" Neuseeland

„Es ist auffällig, dass weiterhin [öffentlich] verfügbare Standard-Malware verwendet wird, was zeigt, dass UAC-0113 [APT29] seine Operationen anpasst und bereit ist, eine Vielzahl von Tools zu verwenden."

Bekannt gegeben am 19. September 2022: Regierung und Privatsektor | „Mehrere geografische Regionen"

Eine APT29 Cyberdefense-Strategie:

Wie Sie APT29-Angriffe vor der Entdeckung oder Löschung entschärfen können

Eindringen in das Netzwerk durch Phishing-Kampagnen oder über kompromittierte Lieferanten.

Hacker zu stoppen, bevor sie in das Netzwerk eindringen, ist der einfachste, billigste und schnellste Weg, jede Geschäftseinheit zu schützen, ohne den Betrieb zu unterbrechen.

- EDR
- Webbasierte Inhalte einschränken
- Antivirus / Antimalware
- Anti-Phishing
- Benutzerschulung und Ausbildung
- Passwortlose MFA
- Benutzerzugriffskontrolle
- Anwendungskontrolle
- Gerätehygiene und -management
- Sicherheitsprogramm-Audits
- Strategische Automatisierung
- Konfigurationsmanagement

Zugriff auf Admin-Profile und / oder Abfangen von Authentifizierungspaketen, um gehackte Berechtigungen zu erhöhen.

Die Einschränkung der Möglichkeiten von Eindringlingen, ihre Anmeldedaten zu erhöhen, hilft, Datendiebstahl und Erpressung zu verhindern.

- Benutzerzugriffskontrolle
- Verwaltung von Privilegien
- Konfigurationsmanagement
- Sicherheitsprogramm-Audits
- Benutzerschulung und Ausbildung

Kartennetz für nützliche Informationen und Schwachstellen.

Wenn sich Eindringlinge nicht frei oder leicht im Netzwerk bewegen können, können sie keine wichtigen Daten oder Sicherheitslücken finden – wasdie Auswirkungen auf das Geschäft verringert.

- Risikobasiertes Patch- und Schwachstellenmanagement
- Gerät und Segmentierung
- Gerätehygiene und -management
- Asset-Abstimmung
- Sichere Zugangsprotokolle
- Segmentierung des Netzes
- Verwaltung von Privilegien
- Strategische Automatisierung
- Konfigurationsmanagement

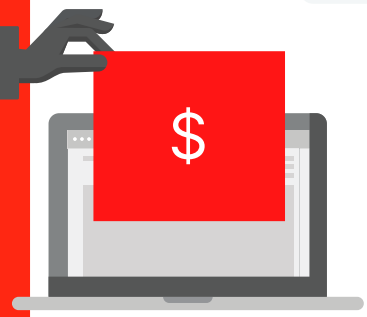
Warten, Daten exfiltrieren und die Angriffsfläche für die Verteidigung vergrößern, wenn sie zum Teil durch das Löschen von Protokollen entdeckt werden.

Ungewöhnliche Verhaltenswarnungen können das Anfangsstadium eines Ransomware-Angriffs signalisieren, bevor der Betrieb eingestellt wird oder Lösegeld gefordert wird.

- Sicherheitsprogramm-Audits
- EDR
- Webbasierte Inhaltsbeschränkungen
- Strategische Automatisierung
- Erkennung und Isolierung bösartiger Verschlüsselungen

Angriff auf Kommando für größte Verwirrung und Wirkung.

Für proaktive Prävention ist es zu spät, Umschalten in den „Disaster Recovery"-Modus.



Conti

Für jeden, der sich mit Cybersicherheit beschäftigt und die neuesten Ransomware-Nachrichten verfolgt, ist „Conti“ ein bekannter Name. Ein weiterer Angreifer, der mit Russland in Verbindung gebracht – wenn auch nicht aktiv von ihm gesponsert – wird, machte im Februar 2022 Schlagzeilen, als er nach der Invasion in der Ukraine seine „volle Unterstützung der russischen Regierung“ ankündigte.

Seit jedoch interne Unzufriedene das Trainingshandbuch der Organisation veröffentlicht und externe Sicherheitsforscher interne Dokumente auf Twitter geleakt haben, scheint sich „Conti“ als einzelne kriminelle Organisation vollständig aufgelöst zu haben.

Da es keine unmittelbaren Nachrichten gibt, die sie zum Handeln zwingen, könnten Stakeholder, die nicht aus dem Bereich InfoSec kommen, Ihre Cybersicherheitsstrategie in Frage stellen, wenn Sie die Conti-Ransomware-Prävention erwähnen – aber Sie wissen, dass dies ein Ablenkungsmanöver ist, das von der tatsächlichen Bedrohung ablenkt.

Wenn Conti nicht mehr da ist, warum sollten sich die Stakeholder für die Verhinderung früherer Angriffe interessieren?

Offen gesagt, hatte Conti eine Zeit lang ein Reputationsproblem – ironischerweise aufgrund seiner eigenen schlechten operativen Sicherheit und internen Moral!

Die Talfahrt begann mit den durchgesickerten Trainingsbüchern für die Conti-Ransomware-Mitglieder. Der letzte Nagel im Sarg kam, als ein anonymer ukrainischer IT-Spezialist in das Netzwerk der Bande eindrang und jahrelanges internes Material durchsickerte.

Aber nur weil Conti „tot“ ist, heißt das nicht, dass seine Hacker nicht mehr aktiv sind oder dass sein Code plötzlich nicht mehr funktioniert.

Conti verfügte über eine umfangreiche Partnerorganisation, die eindeutig darin geschult war, wie man den geschriebenen Ransomware-Code und die Techniken einsetzt, die immer noch eine Bedrohung für jedes Unternehmen mit den noch vorhandenen Sicherheitslücken darstellen.

Und es ist ja nicht so, dass die Hacker, Programmierer und Social Engineers der Conti-Organisation selbst verhaftet wurden oder gestorben sind.

Tatsächlich hat das US-Außenministerium zwei volle Monate nach der Abschaltung der Conti-Server ein neues Video veröffentlicht, in dem es eine Prämie von 10 Millionen Dollar für Informationen auslobt, die zur Verhaftung von „Conti“-Hackern führen.

In letzter Zeit haben Cybersecurity-Forscher und -Analysten Taktiken im Stil von Conti bei anderen Cyberkriminellen beobachtet, darunter:

- BlackByte
- Karakurt
- BlackBasta
- HelloKitty
- AvosLocker
- Hive
- ALPHV – und andere!

Durch die Untersuchung früherer Conti-Vorfälle können proaktive Unternehmen heute eine Vielzahl ähnlicher Angriffe verhindern, die von kleineren Angreifern mit Contis Taktik durchgeführt werden.

Conti Statistikblatt

Aliases:

Nicht mehr verfügbar

Motiv:

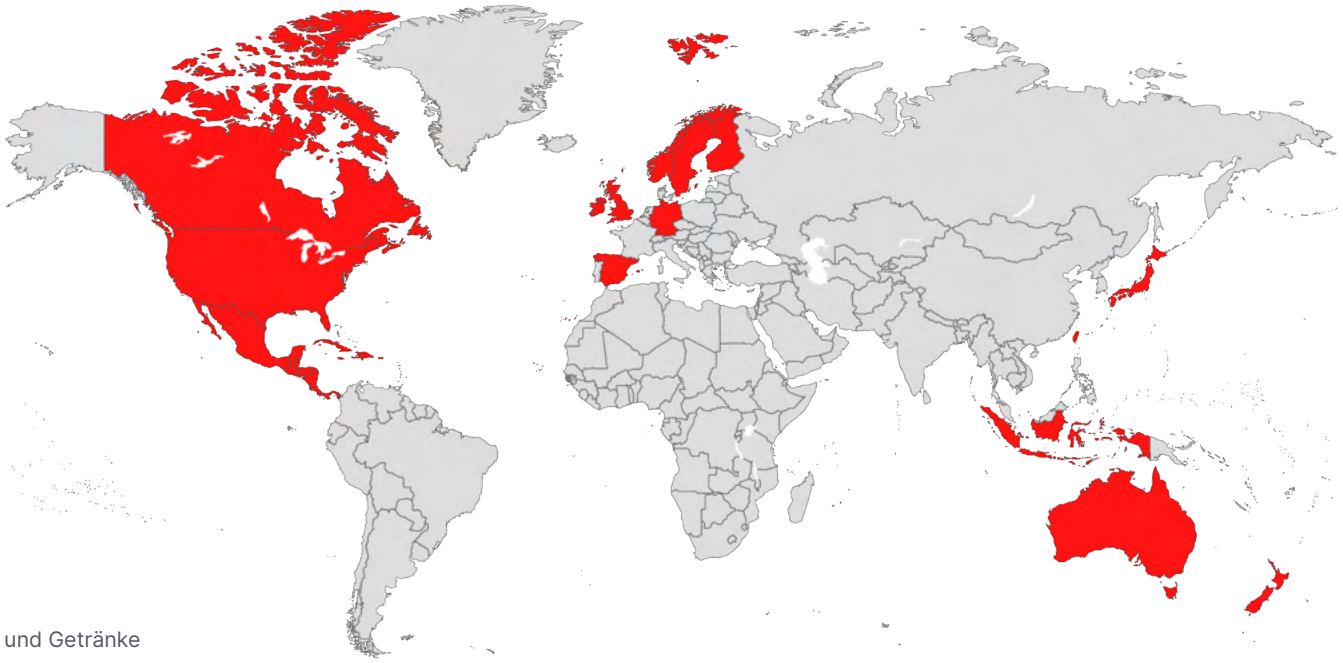
Kriminell / Finanziell

Bedrohungstyp:

Ransomware-as-a-Service (RaaS)

Zugehörigkeit und Verbindungen:

Russland	BlackBasta	Hive
BlackByte	HelloKitty	AvosLocker
Karakurt	ALPHV	Wizard Spider



Kritische Risikobranchen:

Regierung	Gastgewerbe	Lebensmittel und Getränke
Finanzen	Technologie	Einzelhandel & eCommerce
Energie	Gesundheitswesen	
Fertigung	Bildung	

Bevorzugte Exploits:

CVE-2017-0143	CVE-2018-13379	CVE-2021-44228	CVE-2019-1069	CVE-2019-1388	CVE-2021-21972
CVE-2017-0144	CVE-2020-0796	CVE-2015-2546	CVE-2019-1129	CVE-2019-1405	CVE-2021-21985
CVE-2017-0145	CVE-2020-1472	CVE-2016-3309	CVE-2019-1130	CVE-2019-1458	CVE-2021-22005
CVE-2017-0146	CVE-2021-1675	CVE-2017-0101	CVE-2019-1215	CVE-2020-0609	CVE-2021-26855
CVE-2017-0147	CVE-2021-31207	CVE-2018-8120	CVE-2019-1253	CVE-2020-0638	
CVE-2017-0148	CVE-2021-34473	CVE-2019-0543	CVE-2019-1315	CVE-2020-0688	
CVE-2018-12808	CVE-2021-34523	CVE-2019-0841	CVE-2019-1322	CVE-2020-0787	
CVE-2018-13374	CVE-2021-34527	CVE-2019-1064	CVE-2019-1385	CVE-2021-1732	

Bekannte Zielregionen:

Australien	Lateinamerika
Kanada	Neuseeland
Costa Rica	Skandinavien
Deutschland	Spanien
Indonesien	Taiwan
Irland	Vereinigtes Königreich
Japan	Vereinigte Staaten

Auswirkungen ausgewählter Conti-Angriffe auf Unternehmen

Von den 65.000 Computern im Netzwerk von Delta [Electronic] sind etwa 1.500 Server und etwa 12.000 Computer verschlüsselt. [...] Seit dem Vorfall ist fast eine Woche vergangen, und die Delta-Website wurde noch nicht wiederhergestellt.

21. Januar 2022: Delta Electronics Manufacturing | Taiwan

„[...] Conti hatte über 4.000 Geräte und 120 VMware ESXi-Server von Shutterfly verschlüsselt. Eine private Seite mit Datenlecks zeigte auch Beispiele für die von Shutterfly gestohlenen Daten, von denen uns gesagt wurde, dass sie rechtliche Vereinbarungen, Bank- und Händlerkontoinformationen, [...] und anscheinend Kundeninformationen, einschließlich der letzten vier Ziffern von Kreditkarten, enthalten."

Angegriffen am 3. Dezember 2021 – Berichtet am 26. Dezember 2021: Shutterfly | Einzelhandel und eCommerce | Vereinigte Staaten

„Zum jetzigen Zeitpunkt können wir Bestellungen nicht sicher bearbeiten und Waren nicht versenden. Wir haben Teams, die an der Lösung arbeiten, aber es ist nicht bekannt, wann das Problem gelöst sein wird.""

28.01.2022: KP Snacks | Lebensmittel und Getränke Vereinigtes Königreich

„Christian Rucavado, geschäftsführender Direktor der costaricanischen Exporteurskammer, sagte der Angriff auf die Zollbehörde habe die Import- und Exportlogistik des Landes zusammengebrochen Logistik des Landes. Er beschrieb einen Wettlauf mit der Zeit Uhr für verderbliche Waren, die in Kühlhäusern warten, und sagte, man könne die wirtschaftlichen Verluste noch nicht abschätzen."

18. April 2022: Ministerien für Finanzen, Arbeit und soziale Sicherheit Regierung | Costa Rica

„BI weiß, dass im letzten Monat eine Software gehackt wurde. Wir sind uns bewusst, dass wir von einem Cyber-Angriff betroffen sind. Das ist ein Verbrechen, das ist real, und wir sind dem ausgesetzt."

Angegriffen Dezember 2021 – Berichtet 20. Januar 2022: Bank of Indonesia | Finanzen | Indonesien

„Um die Assets der Kunden zu schützen, wurde der Fernzugriff von der IT-Infrastruktur der Nordex-Gruppe für die unter Vertrag stehenden Anlagen deaktiviert. [Das Unternehmen arbeitet weiter an der Wiederherstellung seiner IT-Systeme, um die Kontinuität des Geschäftsbetriebs zu gewährleisten und den normalen Betrieb so bald wie möglich wieder aufzunehmen."

31. März 2022: Nordex | Produktion / Energie | Deutschland

AUSGELÖST im JUNI 2022

Eine Conti Legacy Cyberdefense Strategie:

Wie man Angriffe im Conti-Stil vor der Lösegeldforderung unterbindet

Eindringen in das Netzwerk durch Phishing-Kampagnen, schwache Firewalls und / oder schlecht konfigurierte Server oder Geräte mit Internetanschluss.

Hacker zu stoppen, bevor sie in das Netzwerk eindringen, ist der einfachste, billigste und schnellste Weg, alle Geschäftsbereiche zu schützen, ohne den Betrieb zu unterbrechen.

- EDR
- Webbasierte Inhaltsbeschränkungen
- Antivirus / Antimalware
- Anti-Phishing für Mobiltelefone
- Benutzerschulung und Ausbildung
- Passwortlose MFA
- Benutzerzugriffskontrolle
- Anwendungskontrolle
- Gerätehygiene und -management
- Sicherheitsprogramm-Audits
- Strategische Automatisierung
- Konfigurationsmanagement

Erlangung von Administratorrechten für Hacker-Benutzerkonten, wobei die Aktivitäten als legitim getarnt werden.

Wenn Sie die Möglichkeiten von Eindringlingen einschränken, die Sicherheitsstufe ihrer Anmeldedaten zu erhöhen, können Sie Datendiebstahl und Erpressung verhindern.

- Benutzerzugriffskontrolle
- Verwaltung von Privilegien
- Konfigurationsmanagement
- Sicherheitsprogramm-Audits
- Benutzerschulung und Ausbildung

Kartennetz für strategische Informationen und Schwachstellen.

Wenn sich Eindringlinge nicht frei oder leicht im Netzwerk bewegen können, können sie keine wichtigen Daten oder Sicherheitslücken finden – und so die Auswirkungen auf das Geschäft verringern.

- Risikobasiertes Patch- und Schwachstellenmanagement
- Gerät und Segmentierung
- Gerätehygiene und -management
- Asset-Abstimmung
- Sichere Zugangsprotokolle
- Segmentierung des Netzes
- Verwaltung von Privilegien
- Strategische Automatisierung
- Konfigurationsmanagement

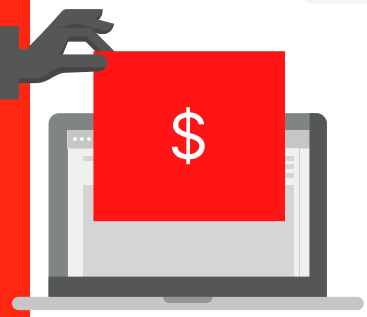
Exfiltrieren von Daten, um sie für Erpressung zu nutzen.

Wenn die Hacker keine Daten stehlen oder sperren können, haben sie kaum ein Druckmittel, um ein Lösegeld zu fordern.

- Sicherheitsprogramm-Audits
- EDR
- Webbasierte Inhaltsbeschränkungen
- Strategische Automatisierung
- Erkennung und Isolierung bösartiger Verschlüsselungen

Start der Ransomware und Erpressungsforderungen mit möglichen DDoS-Angriffen, um die Zahlung zu erzwingen.

Für proaktive Prävention ist es zu spät; wechseln Sie in den „Disaster Recovery"-Modus.



Lapsus$

Wie Conti dachte jeder, dass Lapsus$ mit der Verhaftung seines Anführers – eines 16-jährigen Hackers mit Autismus, der sich „White“ oder „Breachbase“ nennt – durch die Londoner Polizei im März 2022 erledigt sei.

Aber nur ein paar Monate später beschuldigten große Unternehmen die vermeintlich verschwundene Bande mit ihren alten Verstößen. Und dann gerieten ganz neue Infiltrationen bei großen Technologieunternehmen in die Schlagzeilen!

Wie Conti kann diese scheinbar spontane Wiederauferstehung von Lapsus$ als cyberkriminelle Bedrohung Ihnen dabei helfen, Ihre Stakeholder, die nicht aus dem Bereich InfoSec kommen, daran zu erinnern, dass selbst „tote“ Cyberbedrohungen noch abgewehrt werden sollten.

Wir haben jedoch Lapsus$ einbezogen, da die Gruppe eine ganz andere Art von Motivation für Angriffe und Infiltrationsmethoden vertritt.

Wie Sie sehen, scheint Lapsus$ nicht primär durch Geld motiviert zu sein, obwohl sie sicherlich Lösegeld für Informationen fordern und Unternehmen erpressen, damit sie Millionen zahlen.

Stattdessen scheinen die Lapsus$-Hacker aus Neugierde anzugreifen – „Kann ich das überhaupt?“ – und dem uralten Drang junger Menschen nach Aufmerksamkeit mit allen Mitteln.

Warum sollte eine Gruppe jugendlicher Hacker Ihre Stakeholder beunruhigen?

Um Ihre Stakeholder davon zu überzeugen, dass sich Lapsus$-Angriffe im Vergleich zu Avpoid-Angriffen lohnen, müssen Sie zunächst aufzeigen, wie unterschiedlich die Infiltrations- und Angriffsmethoden dieser Teenager sind.

Schließlich verfügten diese Hacker nicht über so viel Geld oder Verbindungen wie unsere anderen vorgestellten Angreifer. Sie hatten nicht die Zeit, sich einem kriminellen Unternehmen zu widmen, wie erwachsene Hacker, deren Vollzeitjob es war, mit kriminellen Aktivitäten Geld zu verdienen.

Stattdessen nutzten die Lapsus$-Hacker die Tools, die ihnen zur Verfügung standen, um Organisationen zu infiltrieren: soziale Medien.

Auf ihrem öffentlichen Telegram-Kanal kündigte Lapsus$ an, dass sie auf der Suche nach ersten Logins und anderen hackbaren Informationen über große Unternehmen und Organisationen seien. Sie wären bereit, Kryptowährungen für die Informationen zu tauschen, wenn der Informant dafür bezahlt werden möchte.

Und verärgerte Mitarbeiter schienen das Angebot tatsächlich zu nutzen.

In den Wochen und Monaten nach dem ersten Telegram-Posting gaben mehrere große Unternehmenöffentlich bekannt, dass sie die Lapsus$-Bande für den Einbruch verantwortlich machen.

Sobald sie sich Zugang zu einem Unternehmen verschafft hatten, bewegten sie sich seitwärts durch das System, soweit sie konnten – und gingen dabei so weit, dass sie intern andere Mitarbeiter und IT-Abteilungen mit den erlangten Anmeldedaten phishten. Sie könnten auf gemeinsam genutzte Laufwerke zugreifen, sich im Hintergrund von Besprechungen aufhalten und unverschlüsselte Kennwortdokumente entdecken.

Dann könnten die Lapsus$-Hacker Daten exportieren, sie löschen und das Chaos von innen heraus beobachten. Sie könnten Lösegeldforderungen über interne Kommunikationskanäle übermitteln!

Wenn die Moral Ihrer Mitarbeiter kritisch niedrig ist und Ihre Nicht-InfoSec-Mitarbeiter ihre eigene Rolle in der Cybersicherheit nicht wahrnehmen, dann stellen sie eine ernsthafte „Insider-Bedrohung“ für die operative Sicherheit Ihres Unternehmens dar – sowohl nach innen als auch nach außen – was sich in lapsus$ Cyberangriffsmustern zeigt.

Lapsus$ Statistikblatt

Aliases:

k. A.

Motiv:

Hacktivisten, Finanziell

Bedrohungstyp:

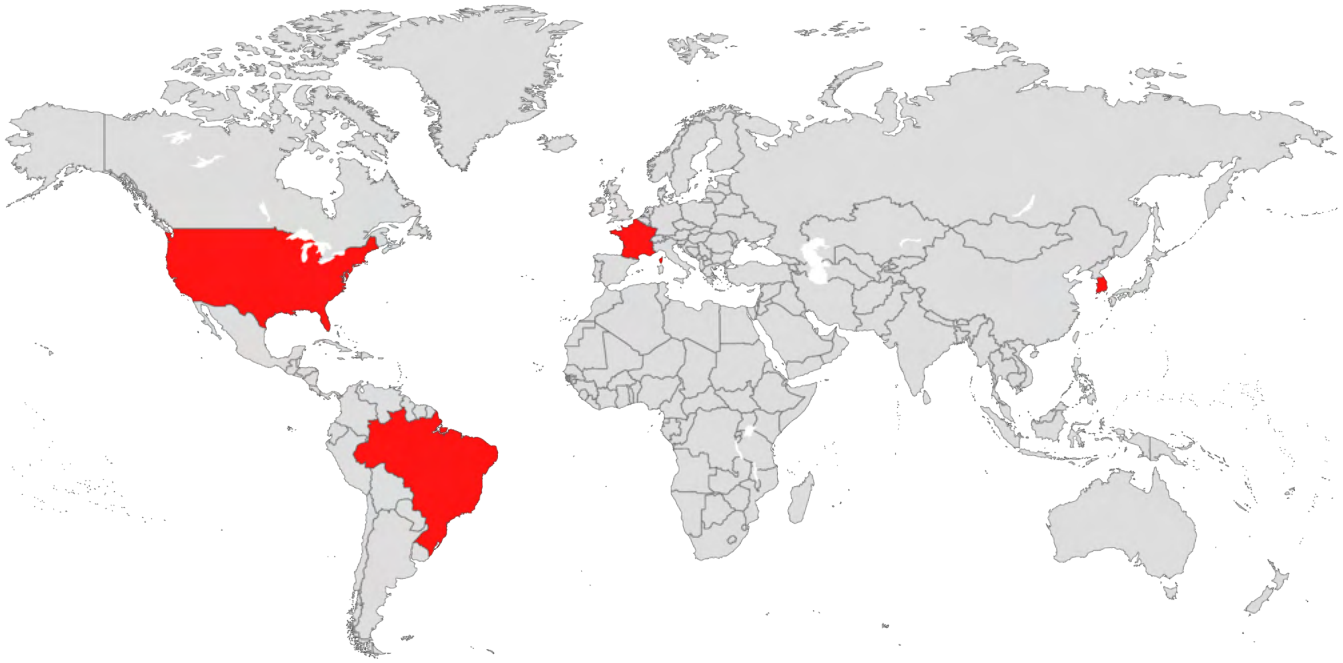
Allgemeine Hacker

Zugehörigkeit und Verbindungen:

UNC2447
Yanluowangr

Kritische Risikobranchen:

Unterhaltung
Technologie



Bevorzugte Exploits:

CVE-2021-34484
CVE-2018-13379
CVE-2020-12812
CVE-2020-23852
CVE-2021-26857
CVE-2021-31207
CVE-2021-44864
CVE-2021-44957
CVE-2021-45326
CVE-2021-45328
CVE-2022-0510
CVE-2022-21702
CVE-2022-0139
CVE-2021-45327
CVE-2021-45325
CVE-2021-44956
CVE-2021-34473
CVE-2021-26858
CVE-2021-26855
CVE-2020-23705
CVE-2019-5591
CVE-2021-34484
CVE-2022-21919
CVE-2022-26904
CVE-2021-34484

Bekannte Zielregionen:

Brasilien
Frankreich
Südkorea
Vereinigte Staaten

Auswirkungen ausgewählter Lapsus$-Angriffe auf dasUnternehmen

Der Angreifer versuchte dann wiederholt, sich in das Uber-Konto des Vertragspartners einzuloggen. Jedes Mal erhielt der Auftragnehmer eine Genehmigungsanfrage für den Zwei-Faktor-Login, die den Zugang zunächst blockierte. Schließlich akzeptierte der Vertragspartner jedoch einen und der Angreifer konnte sich erfolgreich einloggen.

15. September 2022: Uber | Technologie | Vereinigte Staaten

„Ich bin sehr enttäuscht über die lange Zeitspanne, die zwischen unserer Meldung an [Firma] und der Herausgabe des vollständigen Untersuchungsberichts vergangen ist. Wenn ich darüber nachdenke, hätten wir nach Erhalt des zusammenfassenden Berichts der Firma schneller handeln sollen, um seine Auswirkungen zu verstehen.

Januar 2022: Okta | Technologie | Vereinigte Staaten

„Nach unserer ersten Analyse betrifft der Verstoß einige Quellcodes, die sich auf den Betrieb von Galaxy-Geräten beziehen, aber nicht die persönlichen Daten unserer Kunden oder Mitarbeiter.

Angekündigt am 3. März 2022: Samsung | Elektronik / Fertigung | Südkorea

Am 11. September 2022 haben die Täter, die zuvor eine Liste von Dateinamen aus diesem Sicherheitsvorfall im Dark Web veröffentlicht hatten, die tatsächlichen Inhalte der gleichen Dateien an derselben Stelle im Dark Web veröffentlicht.“

Angriff 24. Mai 2022 – Berichtet 10. August 2022: Cisco Electronics / Fertigung | Vereinigte Staaten

Wir wissen, dass der Angreifer [Lapsus$] Anmeldedaten von Mitarbeitern und einige geschützte Informationen von Nvidia von unseren Systemen entwendet hat und damit begonnen hat, diese online zu verbreiten.“

23. Februar 2022: Nvidia | Elektronik / Fertigung | Südkorea

„Bei der Veröffentlichung des Torrents sagte Lapsus$, er enthalte 90 % des Quellcodes für Bing und etwa 45 % des Codes für Bing Maps und Cortana.

20. März 2022: Microsoft | Technologie | Vereinigte Staaten

„Vor kurzem sind wir Opfer eines Netzwerkeinbruchs geworden, bei dem sich ein unbefugter Dritter illegal Zugang zu unseren Systemen verschafft und vertrauliche Informationen heruntergeladen hat, darunter auch frühes Entwicklungsmaterial für das nächste Grand Theft Auto.“

19. September 2022: Rockstar Games | Entertainment | Vereinigte Staaten

Ihre Lapsus$ Cyberdefense Strategie:

Wie Sie Lapsus$-Angriffe vor Vandalismus oder Löschung unterbinden

Eindringen in das Netzwerk über die Anmeldeinformationen von Insidern sowie über die persönlichen Konten der Mitarbeiter als „Hintertür“ zum Netzwerk des Arbeitgebers.

Hacker zu stoppen, bevor sie in das Netzwerk eindringen, ist der einfachste, billigste und schnellste Weg, alle Geschäftsbereiche zu schützen, ohne den Betrieb zu unterbrechen.

- Benutzerzugriffskontrolle
- Verwaltung von Privilegien
- Sicherheitsprogramm-Audits
- Anwendungskontrolle
- Passwortlose MFA
- Segmentierung des Netzes
- Benutzerschulung und Ausbildung
- Strategische Automatisierung

Suchen Sie nach exponierten Zugangsdaten in offenen, gemeinsam genutzten Datenbanken oder durch interne Social Engineering-Angriffe von innen.

Die Einschränkung der Möglichkeiten von Eindringlingen, Anmeldedaten zu ändern oder zu erhöhen, hilft, Datendiebstahl und Erpressung zu verhindern.

- Benutzerzugriffskontrolle
- Verwaltung von Privilegien
- Sicherheitsprogramm-Audits
- Anwendungskontrolle
- Passwortlose MFA
- Segmentierung des Netzes
- Benutzerschulung und Ausbildung
- Strategische Automatisierung

Extrahieren von Daten entweder um Berühmtheit zu erlangen (proff oder hack0) oder für zukünftige Erpressungen.

Wenn die Hacker keine Daten stehlen können, haben sie kaum ein Druckmittel, um ein Lösegeld zu fordern.

- Eingeschränkte webbasierte Inhalte
- Benutzerzugriffskontrolle
- Verwaltung von Privilegien
- Segmentierung des Netzes
- Anwendungskontrolle
- EDR
- Sicherheitsprogramm-Audits
- Strategische Automatisierung
- Gerätehygiene und -management

Beginn der Erpressung – möglicherweise über die internen Kanäle des Opfers! – wenn dasUnternehmenmit der Reaktion auf den Vorfall beginnt.

Für proaktive Prävention ist es zu spät, Umschalten in den „Disaster Recovery“-Modus.

Der InfoSec Tactical Index

ivanti CSW Cyber SecurityWorks

Der InfoSec Tactical Index

In diesem Abschnitt

ALPHV MITRE ATT&CK Karte

1. Aufklärung

T1595: Aktives Scannen
T1589: Erfassen von Informationen zur Identität des Opfers
  T1589.001: Anmeldeinformationen

2. Ressourcenentwicklung

k. A.

3. Ursprünglicher Zugang

T1078: Gültige Konten
T1190: Exploit von öffentlich zugänglicher Anwendung

4. Ausführung

k. A.

5. Persistenz

T1098: Kontomanipulation

6. Privilegienerweiterung

T1548: Mechanismus zur Kontrolle von Missbrauchseskalation
  T1548.002: Umgehung der Benutzerkontensteuerung

7. Ausweichen der Verteidigung

T1564: Artefakte verstecken

8. Zeugnis-Artefakte

T1003: OS Credential Dumping
  T1003.001: LSASS-Speicher
  T1003.004: LSA-Geheimnisse

9. Entdeckung

T1082: Ermittlung von Systeminformationen
T1135: Erkennung von Netzwerkfreigaben
T1018: Entfernte Systemermittlung
T1087: Kontoerfassung
  T1087.002: Domain-Konto
T1487: Entdeckung von Domain Trusts
T1057: Prozess-Entdeckung
T1083: Datei- und Verzeichnisrecherche

10. Seitwärtsbewegung

T1563: Remote Service Hijacking
  T1563.002: RDP-Hijacking
T1570: Lateral Tool Transfer

11. Sammlung

T1005: Daten vom lokalen System

12. Kommando und Kontrolle

T1090: Proxy
  T1090.003: Multi-hop Proxy

13. Exfiltration

T1567: Exfiltration über Webservice
  T1567.002: Exfiltration zum Cloud-Speicher

14. Auswirkungen

T1486: Verschlüsselte Daten für stärkere Auswirkungen
T1489: Service Stop
T1490: Systemwiederherstellung unterbinden

APT29 MITRE ATT&CK Karte

1. Aufklärung

k. A.

2. Ressourcenentwicklung

T1583: Erwerben von Infrastruktur
- T1583.001: Domains
- T1583.006: Web Services

T1584: Infrastruktur kompromittieren
- T1584.001: Domains

T1587: Entwicklung von Fähigkeiten
- T1587.001: Malware
- T1587.003: Digitale Zertifikate

3. Ursprünglicher Zugang

T1078: Gültige Konten
- T1078.002: Domain-Konten

T1133: Externe Remote-Dienste

T1190: Exploit von öffentlich zugänglicher Anwendung

T1195: Kompromittierung der Lieferkette
- T1195.002: Kompromittierung der Softwarelieferkette

T1566: Phishing
- T1566.001: Spearphishing-Anhang
- T1566.002: Spearphishing-Link

4. Ausführung

T1047: Windows-Verwaltungsinstrumentierung

T1204: Benutzer-Ausführung
- T1204.001: Bösartiger Link
- T1204.002: Bösartige Datei

T1053: Geplanter Task/Job
- T1053.005: Geplante Aufgabe

T1059: Befehls- und Scripting-Interpreter
- T1059.001: PowerShell
- T1059.003: Windows-Befehlsshell
- T1059.006: Python

T1203: Ausnutzung für Client-Ausführung

5. Persistenz

T1053: Geplanter Task/Job
- T1053.005: Geplante Aufgabe

T1078: Gültige Konten
- T1078.002: Domain-Konten

T1098: Kontomanipulation
- T1098.001: Zusätzliche Cloud-Berechtigungsnachweise
- T1098.002: Zusätzliche Berechtigungen für E-Mail-Delegierte

T1133: Externe Remote-Dienste

T1546: Ereignisausgelöste Ausführung

T1546.003: Windows Mangement Instrumentation Ereignisabonnement

T1546.008: Zugänglichkeitsmerkmale

6. Privilegienerweiterung

T1053: Geplanter Task/Job
- T1053.005: Geplante Aufgabe

T1078: Gültige Konten
- T1078.002: Domain-Konten

T1484: Änderung der Domänenpolitik
- T1484.002: Domain Trust Benachrichtigung

T1546: Ereignisausgelöste Ausführung
- T1546.003: Windows Management Instrumentation Ereignisbeschreibung
- T1546.008: Zugänglichkeitsmerkmale

T1547: Boot- oder Anmelde-Autostart-Ausführung
- T1547.009: Shortcut-Modifikation

7. Ausweichen der Verteidigung

T1027: Verdeckte Dateien oder Informationen
- T1027.002: Software-Paketierung

T1036: Maskerade
- T1036.004: Maskeraden-Task oder -Dienst
- T1036.005: Abgleich mit rechtmäßigem Namen oder Ort

T1070: Entfernen des Indikators auf dem Host
- T1070.004: Datei-Löschung
- T1070.006: Zeitstempel

T1078: Gültige Konten
- T1078.002: Domain-Konten

T1140: Dateien oder Informationen entschlüsseln/dekodieren

T1218: Binäre Proxy-Ausführung des Systems
- T1218.011: Rundll32

T1484: Änderung der Domänenpolitik
- T1484.002: Domain Trust-Benachrichtigung

T1548: Mechanismus zur Kontrolle der Missbrauchseskalation
- T1548.002: Umgehung der Benutzerkontensteuerung

T1550: Verwendung von alternativem Authentifizierungsmaterial
- T1550.003: Ticket weitergeben
- T1550.004: Web Session Cookie

T1553: Untergrabung der Vertrauenskontrollen
- T1553.002: Code-Signierung

T1562: Beeinträchtigung der Verteidigung
- T1562.001: Deaktivieren oder Ändern von Tools
- T1562.002: Deaktivierung der Windows-Ereignisprotokollierung
- T1562.004: Deaktivieren oder Ändern der System-Firewall

8. Zugang zu Anmeldeinformationen

T1003: OS Credential Dumping
- T1003.006: DCSync

T1005: Daten vom lokalen System

T1552: Ungesicherte Zugangsdaten
- T1552.004: Private Schlüssel

T1555: Anmeldeinformationen aus Passwortspeichern

T1558: Kerberos-Tickets stehlen oder fälschen
- T1558.003: Kerberoroasting

T1606: Web-Anmeldeinformationen fälschen:
- T1606.001: Web Cookies
- T1606.002: SAML Tokens

9. Entdeckung

T1016: Erkennung der Systemnetzwerkkonfiguration
- T1016.001: Ermittlung der Internetverbindung

T1018: Entfernte Systemermittlung

T1057: Prozessentdeckung

T1069: Erkennung von Berechtigungsgruppen

T1082: Ermittlung von Systeminformationen

T1083: Datei- und Verzeichnisrecherche

T1087: Kontoerfassung

T1482: Entdeckung von Domain Trusts

10. Seitwärtsbewegung

T1021: Remote-Dienste
- T1021.006: Windows-Fernverwaltung

T1550: Verwendung von alternativem Authentifizierungsmaterial
- T1550.003: Ticket weitergeben
- T1550.004: Web Session Cookie

11. Sammlung

T1074: Daten gestaged
- T1074.002: Fernsignierung von Daten

T1114: E-Mail-Abholung
- T1114.002: Remote E-Mail-Abholung

T1560: Archivierung gesammelter Daten
- T1560.001: Archivieren über Dienstprogramm

12. Kommando und Kontrolle

T1001: Datenverschleierung
- T1001.002: Datenverschleierung: Steganographie

T1071: Protokolle der Anwendungsebene
- T1071.001: Web-Protokolle

T1090: Proxy
- T1090.001: Interner Proxy
- T1090.003: Multi-hop Proxy
- T1090.004: Domain-Fronting

T1095: Protokoll für die Nicht-Anwendungsebene

T1102: Web-Dienst
- T1102.002: Bidirektionale Kommunikation

T1105: Ingress-Tool-Transfer

T1568: Dynamische Auflösung

13. Exfiltration

T1048: Exfiltration über ein alternatives Protokoll
- T1048.002: Exfiltration über asymmetrisch verschlüsseltes Nicht-C2-Protokoll

14. Auswirkungen

k. A.

Conti MITRE ATT&CK Karte

1. Aufklärung

T1595: Aktives Scannen

2. Ressourcenentwicklung

k. A.

3. Ursprünglicher Zugang

T1190: Exploit von öffentlich zugänglicher Anwendung
T1566: Phishing
- T1566.001: Spearphishing-Anhang
- T1566.002: Spearphishing-Link
- T1566.003: Spearphishing über Service

4. Ausführung

T1072: Tools für die Softwarebereitstellung
T1203: Exploit für Client-Ausführung

5. Persistenz

T1037: Skripte zur Initialisierung von Boor oder Logon
T1542: Pre-OS Boot
T1542.003: Bootkit
T1543: Erstellen oder Ändern von Systemprozessen
- T1543.001: Launch Agent
- T1543.002: System-Service
- T1543.003: Windows-Service
- T1543.004: Launch Daemon

T1546: Ereignisausgelöste Ausführung
- T1546.001: Standard-Dateizuordnung ändern
- T1546.004: Änderung der Unix-Shell-Konfiguration
- T1546.008: Accessibility-Features

T1547: Boot- oder Anmelde-Autostart-Ausführung
- T1547.006: Kernel-Module und Execution Flow
- T1547.009: Shortcut-Modifikation

T1574: Hijacken des Execution Flow
- T1574.008: Path Interception durch Hijacking von Suchaufträgen
- T1574.009: Shortcut-Modifikation
- T1574.010: Schwachstellen bei den Berechtigungen für Servicedateien
- T1574.011: Schwachstelle in der Diensteregistrierung

6. Privilegienerweiterung,

T1037: Skripte zur Initialisierung von Boor oder Logon
T1055: Prozessinjektion
T1134: Zugriffstoken-Manipulation
T1543: Erstellen oder Ändern von Systemprozessen
- T1543.001: Launch Agent
- T1543.002: Systemservice
- T1543.003: Windows-Service
- T1543.004 Launch Daemon

T1546: Ereignisausgelöste Ausführung
- T1546.001: Standard-Dateizuordnung ändern
- T1546.004: Änderung der Unix-Shell-Konfiguration
- T1546.008: Accessibility-Features

T1547: Boot- oder Anmelde-Autostart-Ausführung
- T1547.006: Kernel-Module und Execution Flow
- T1547.009: Shortcut-Modifikation

T1548: Mechanismus zur Kontrolle von Missbrauchseskalation
T1574: Hijacken des Execution Flow
- T1574.010: Schwachstellen bei den Berechtigungen für Servicedateien
- T1574.011: Schwachstelle in der Diensteregistrierung

7. Ausweichen der Verteidigung

T1027: Verdeckte Dateien oder Informationen
- T1027.003: Steganographie

T1014: Rootkit
T1036:Maskerade
- T1036.005: Abgleich mit rechtmäßigem Namen oder Ort

T1055: Prozess-Injektion
T1112: Ändern der Registrierung
T1134: Zugriffstoken-Manipulation
T1218: Signierte binäre Proxy-Ausführung
- T1218.001: Kompilierte HTML-Datei

T1542: Pre-OS Boot
- T1542.003: Bootkit
- T1542.004: Installieren des Root-Zertifikats

T1548: Mechanismus zur Kontrolle von Missbrauchseskalation
T1553: Untergrabung der Vertrauenskontrollen
T1562: Beeinträchtigung der Verteidigung
- T1562.001: Deaktivieren oder Ändern von Tools

T1574: Hijacken des Execution Flow
- T1574.010: Schwachstelle bei den Servicedateirechten
- T1574.011: Dienste-Registrierungsberechtigungen

8. Zugang zu Anmeldeinformationen

T1005: Tools für die Softwarebereitstellung
T1080: Beschädigung gemeinsamer Inhalte

9. Sammlung

T1005: Daten vom lokalen System
T1039: Daten vom freigegebenen Netzlaufwerk
T1115: Zwischenablage-Daten
T1123: Audioaufnahme
T1125: Videoaufnahme

10. Kommando

k. A

11. Exfiltration

T1020: Automatisierte Exfiltration
- T1020.001: Traffic-Duplizierung

12. Auswirkungen

T1498: Denial of Service im Netzwerk
- T1498.001: Direkte Netzwerküberflutung

Lapsus$ MITRE ATT&CK Karte

1. Aufklärung

k. A.

2. Ressourcenentwicklung

k. A.

3. Ursprünglicher Zugang

T1078: Gültige Konten
T1133: Externe Remote-Dienste
T1190: Exploit von öffentlich zugänglicher Anwendung
T1199: Vertrauensvolle Beziehung

4. Ausführung

T1059: Geplante Aufgabe
  T1059.001: PowerShell
  T1059.003: Windows-Befehlsshell
  T1059.004: Unix Shell
T1072: Tools für die Softwarebereitstellung

5. Privilegienerweiterung

T1068: Ausnutzung für Privilegieneskalation
T1078: Gültige Konten
  T1078.002: Domain-Konten

6. Persistenz

T1021: Dienste
  T1021.001: Remote Desktop Protokoll
T1078: Gültige Konten
  T1078.002: Domain-Konten
  T1078.003: Lokale Konten
  T1078.004: Cloud-Konten
T1114: E-Mail-Abholung
  T1114.003: Regel für E-Mail-Weiterleitung
T1133: Externe Remote-Dienste

7. Ausweichen der Verteidigung

T1027: Verdeckte Dateien oder Informationen
  T1027.002: Software-Paketierung
T1078: Gültige Konten
  T1078.002: Domain-Konten
  T1078.003: Lokale Konten
  T1078.004: Cloud-Konten
T1553: Untergrabung der Vertrauenskontrollen
  T1553.002: Code-Signierung
T1562: Beeinträchtigung der Verteidigung
  T1562.001: Deaktivieren oder Ändern von Tools

8. Zugang zu Anmeldeinformationen

T1003: OS Credential Dumping
  T1003.001: LSASS-Speicher
T1111: Abfangen der Zwei-Faktor-Authentifizierung
T1212: Ausnutzung für den Zugriff auf Zugangsdaten
T1528: Entwendung von Zugriffstoken für Anwendungen
T1552: Ungesicherte Zugangsdaten
  T1552.001: Anmeldeinformationen in Dateien
  T1552.004: Private Schlüssel
T1555: Anmeldeinformationen aus Passwortspeichern
  T1555.005: Passwort-Manager

9. Entdeckung

T1016: Erkennung der Systemnetzwerkkonfiguration
  T1016.001: Ermittlung der Internetverbindung
T1069: Gruppen-Entdeckung
  T1069.002: Domain-Gruppen
T1082: Ermittlung von Systeminformationen
T1482: Entdeckung von Domain Trusts

10. Seitwärtsbewegung

T1021: Dienste
  T1021.001: Remote Desktop Protokoll
T1534: Internes Spearphishing
T1078: Gültige Konten
  T1078.002: Domain-Konten

11. Sammlung

T1039: Daten vom freigegebenen Netzlaufwerk
T1114: E-Mail-Abholung
  T114.003: Regel für E-Mail-Weiterleitung
T1213: Daten aus Informations-Repositories
  T1213.002: Sharepoint
  T1213.003: Code-Repositories

12. Exfiltration

T114: E-Mail-Abholung
  T1114.003: Regel für E-Mail-Weiterleitung
T1537: Datentransfer in ein Cloud-Konto
T1567: Exfiltration über Webservice

13. Auswirkungen

T1485: Datenvernichtung
T1529: Herunterfahren/Neustart des Systems

Referenzen und Quellen

Neben allen hier aufgeführten Analysten, Berichterstattern und Organisationen gilt unser besonderer Dank den Forschern und internen Experten von Cyber Security Works und Ivanti, die uns Zugang zu Branchenkenntnissen und geschützten Informationen verschafft haben, die dieses Tool Kit erst möglich gemacht haben.

NIST, „Advanced Persistent Threat."

„2022 Global Threat Report." Crowdstrike.

„Alert (AA22-047A): Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology." Cybersecurity & Infrastructure Security Agency (CISA).

„APT29." MITRE ATT&CK.

„Cisco Data Breach Attributed to Lapsus$ Ransomware Group." Dark Reading. „Cisco Event

Response: Corporate Network Security Incident." Cisco Security.

„CISCO Talos shares insights related to recent cyber attack on Cisco." Cisco Talos.

„DEV-0537 criminal actor targeting organizations for data exfiltration and destruction." Microsoft Security.

"„Encevo Cyberattack." Encevo.

„Experts Call the Conti Ransomware Gang Who Broke BI Dangerous Hackers." CNN Indonesia.

„General Security Advisory: Understanding and preparing for cyber threats relating to tensions between Russia and Ukraine." National Cyber Security Centre (NCSC).

„Globant official update." Globant.

„Hacker attack on the province of Carinthia: „Black Cat" wants five million dollars in Bitcoin." DerStandard.

„Incident and Agency Updates." Fremont County Colorado.

„Lapsus$: An In-Depth Look at Data Extortion Group." Avertium.

„MITRE Mapping of CISA KEVs and its Challenges." Cyber Security Works.

„Moncler Press Release - Update on Malware Attack." Moncler Group.

„Nordex Group impacted by cyber security incident." The Nordex Group.

„RE: NOTICE OF DATA BREACH." Meyer Corporation.

„RESPONSE TO LATEST MEDIA REPORTS ABOUT 27 NOVEMBER CYBER SECURITY INCIDENT." CS Energy.

„Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor

Authentication Protocols and „PrintNightmare" Vulnerability." Cyber & Infrastructure Security Agency (CISA).

„Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine." Insikt Group: Recorded Future.

„Security update." Uber Newsroom.

„STATEMENT ABOUT CYBERSECURITY INCIDENT: DECEMBER 26, 2021." Shutterfly, Inc.

„Statement from Oiltanking GmbH Group and Mabanaft GmbH & Co. KG Group." Mabanaft Communications.

„Threat Report: T3 2021." ESET Security Research.

„Ubisoft Cyber Security Incident Update." Ubisoft.

„Update on cyber security incident." The Nordex Group.

Abrams, Lawrence. „Lapsus$ hackers leak 37GB of Microsoft's alleged source code." Bleeping Computer.

Abrams, Lawrence. „Shutterfly discloses data breach after Conti ransomware attack." Bleeping Computer.

Amitai Cohen via @AmitaiCo.

Australian Cyber Security Centre (ACSC). „2021-010: ACSC Ransomware Profile – Conti."

Batra, Anirudh. „Detailed Analysis of LAPSUS$ Cybercriminal Group that has Compromised Nvidia, Microsoft, Okta, and Globant." CloudSEK.

Bill Demirkapi via @BillDemirkapi.

Bradbury, David. „Updated Okta Statement on LAPSUS$." Okta.

Brett Callow via @BrettCallow.

Brown, David; Matthews, Michael; Smallridge, Rob. „LAPSUS$: Recent techniques, tactics and procedures." nncgroup.

Burgess, Matt. „The Workaday Life of the World's Most Dangerous Ransomware Gang." Wired.

Cimpanu, Catalin. „Disgruntled ransomware affiliate leaks the Conti gang's technical manuals." The Record.

Clark, Mitchell. „Nvidia says its 'proprietary information' is being leaked by hackers." The Verge. conti leads via @ContiLeaks.

CÓRDOBA, Javier; Sherman, Christopher. „Cyber attack causes chaos in Costa Rica government systems." AP News.

Culafi, Alexander. „AdvIntel: Conti rebranding as several new ransomware groups." SearchSecurity.

Cyberpedia. „What is the MITRE ATT&CK Framework?" Cortex.

DarkFeed via @ido_cohen2.

DarkTracer : DarkWeb Criminal Intelligence via @darktracer_int.

Davis, Griffin. „‚GTA 6' Leaker Arrested! Authorities Claim Teenager is Linked to Lapsus$ Hacking Group." Tech Times.

Digital Security Unit. „Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine." Microsoft.

DISSENT. „AlphaV claims attack on Florida International University (updated)." DataBreaches.net.

Fadilpašić , Sead. „Conti ransomware group officially shuts down – but probably not for long." techradar.pro.

Fardkhmanesh, Megan. „The Real Impact of the Grand Theft Auto and Diablo Leaks." Wired.

Fox, Barbara. „Fremont County government services closed due to a cyber security breach." KRDO News.

Ganti, Anil. „Samsung says your personal info wasn't leaked in its recent data hack." SamMobile.

Greenberg, Andy (2019) Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.

Greenberg, Andy. „Destructive Hacks Against Ukraine Echo Its Last Cyberwar." Wired.

Greig, Jonathan. „BlackCat ransomware group claims attack on Florida International University." The Record.

Greig, Jonathan. „Louisiana authorities investigating ransomware attack on city of Alexandria." The Record.

Greig, Jonathan. „North Carolina A&T hit with ransomware after ALPHV attack." The Record.

Gupta, Surojoy. „All About Conti." Cyber Security Works.

Gurevich, M (1961) The Social Structure of Acquaintanceship Networks, Cambridge, MA: MIT Press

Harbison, Mike; Renals, Peter. „Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive." Unit 42, Palo Alto Networks.

Hill, Michael. „Cisco admits hack on IT network, links attacker to LAPSUS$ threat group." CSO.

Jenkins, Luke; Hawley, Sarah; Najafi, Parnian; Bienstock, Doug. „Suspected Russian Activity Targeting Government and Business Entities Around the Globe." Mandiant.

Kabelka, Laura. „Austria's Carinthia halts passport issuance over ransomware attack." Euractiv.

Kan, Michael. „Nvidia Confirms Company Data Was Stolen in Hack." PC Mag.

Koczwara, Michael. „LAPSUS$ TTPs."

Lakshmanan, Ravie. „Uber Blames LAPSUS$ Hacking Group for Recent Security Breach." The Hacker News.

Lakshmanan, Ravie. „Uber Claims No Sensitive Data Exposed in Latest Breach... But There's More to This." The Hacker News.

Lyngaas, Sean. „I can fight with a keyboard': How one Ukrainian IT specialist exposed a notorious Russian ransomware gang." CNN.

Mari, Angelica. „Brazilian Ministry of Health suffers cyberattack and COVID-19 vaccination data vanishes." ZDNet.

Meta / Facebook, „Three and a half degrees of separation."

Minggeng, Liu. „Exclusive / Delta was hacked and extorted 410 million yuan, estimated about 13,500 computers were encrypted." CTWant News.

Newman, Lily Hay. „The Dire Warnings in the Lapsus$ Hacker Joyride." Wired.

Panettieri, Joe. „Lapsus$ Cyberattack vs Okta, Sitel: Up to 366 Okta Customers Impacted." MSSP Alert.

Pearson, James. „UPDATE 4-Shell re-routes oil supplies after cyberattack on German firm." Reuters.

Peters, Jay. „Ubisoft says it experienced a 'cyber security incident', and the purported Nvidia hackers are taking credit." The Verge.

Pink, Bidara. „Last month Bank Indonesia (BI) was hit by a cyber attack, but it has been resolved." Kontan Indonesia.

Polityuk, Pavel. „EXCLUSIVE Ukraine suspects group linked to Belarus intelligence over cyberattack." Reuters.

Ransomware Index Update: Q2-Q3 2022. Cyber Security Works, Ivanti.

Ravindran, Priya. „All about BlackCat (ALPHV)." Cyber Security Works.

Rewards for Justice via @RFJ_USA.

Rockstar Games via @RockstarGames.

Scullion, Chris. „Bandai Namco confirms it's been hacked and says it's investigating damage." VGC News.

Sharma, Ax. „KP Snacks giant hit by Conti ransomware, deliveries disrupted.

Soloman, Howard. „Canadian military provider suffered ransom attack, says news report."

Soloman, Howard. "Canadian military provider suffered ransom attack, says news report."

Taipei, Peng Yuwen. „Delta's servers were hacked, and some system recovery operations are estimated to have no major impact." Yahoo News: Taiwan.

Temple-Raston, Dina. „A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack." NPR.

The Reliants Project, „Six Degrees of Kevin Bacon."

Tidy, Joe. „Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal." BBC News.

Todd MicKinnon via @toddmckinnon.

Uchill, Joe. „Globant confirms falling victim to Lapsus$ extortion group." SC Magazine.

Wadhwani, Sumeet. „Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members." spiceworks.

Wadhwani, Sumeet. „Ransomware Group Lapsus$ Cries Foul After NVIDIA Allegedly Does a Tit-for-Tat." spiceworks.

Werkmeister, Luke. „Ripple effects of ransomware attack against Suffolk County continue more than a week later." The Suffolk Times.

Wolfram, John; Hawley, Sarah; McLellan, Tyler; Simonian, Nick; Veilby, Anders. „Trello From the Other Side: Tracking APT29 Phishing Campaigns." Mandiant.

Zetter, Kim (2015) Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.

2023 Cyberstrategy Tool Kit für internes Buy-In

Wie Sie Budgets gewinnen und Stakeholder beeinflussen, indem Sie Außenstehenden in Sachen InfoSec die Bedeutung Ihrer Cybersicherheitsstrategie erklären

in collaboration with

CSW Cyber SecurityWorks

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com