FRÜHER SCHON AN SPÄTER DENKEN

Tatort Cyberattacke:
So schützen sich Unternehmen vor Umsatzausfällen und Verlusten

valantic

Liebe Leserin, lieber Leser,

als erfahrener Breach Coach und Cybersecurity-Berater werde ich von Unternehmen oft um Rat gefragt, wenn die Hütte bereits lichterloh brennt. Dann ist der Worst Case eingetreten und das gängige Szenario, das mein Team und ich vorfinden, sieht so aus: Ein Cyberangriff war erfolgreich und hat für das Unternehmen sehr weitreichende Folgen. Umsatzrelevante IT-Systeme und Geschäftsprozesse fallen – meist komplett – aus. Nichts geht mehr.

Die oberste Priorität der angegriffenen Unternehmen liegt selbstverständlich darauf, die betroffenen Systeme so schnell wie möglich wieder ans Laufen zu bringen. Der naheliegende Ansatz, die gesamte kompromittierte IT wie auf einer grünen Wiese neu aufzubauen, ist unserer Erfahrung nach jedoch sehr zeitaufwändig und kostenintensiv. Und jeder ausgefallene Tag geht enorm ins Geld.

In diesem Whitepaper möchten wir ihnen daher eine smartere, schnellere und trotzdem sichere Alternative vorstellen, die monetären Folgen einer Cyberattacke zu minimieren und den gewohnten Geschäftsbetrieb so schnell wie möglich wieder aufzunehmen. Wir sprechen aus Erfahrung und haben diese Methode in den letzten Jahren bei vielen angegriffenen Unternehmen mit großem Erfolg umgesetzt.

Heute schon an morgen denken

Vor allem Präventionsmaßnahmen können Umsatzausfällen und Verlusten wirksam vorbeugen. Denn die beste Antwort auf einen Cyberangriff besteht ohne Zweifel darin, es gar nicht erst zu einem Angriff kommen zu lassen. Als wirksame Schutzmaßnahme hat sich das sogenannte Darknet Monitoring bewährt, das Angriffe von Cyberkriminellen bereits im Vorfeld erkennen kann. Auch dazu erfahren Sie in diesem Whitepaper viele wichtige Details.

Falls dennoch Fragen offengeblieben sind, kontaktieren Sie mich gerne. Für eine Erstberatung und eine Bedrohungsanalyse stehen mein Team und ich ihnen sehr gerne mit Rat und Tat zur Seite.

Bis dahin verbleibe ich und wünsche allen Leserinnen und Lesern eine spannende, nützliche und inspirierende Lektüre.

Herzlich, Ihr Thomas Lang

Thomas Lang
Partner & Managing Director

+49 6103 5086-0
thomas.lang@mc.valantic.com
www.valantic.com

Inhalt

Die aktuelle Situation

Cybersicherheit befasst sich mit dem Schutz von Computersystemen, Netzwerken und Daten vor digitalen Bedrohungen. Dabei geht es nicht nur um den Schutz vor unerlaubten Zugriffen, sondern auch darum, die Integrität, Verfügbarkeit und Vertraulichkeit von Daten zu gewährleisten. Die Gefahren, denen sich Unternehmen gegenüberstehen, reichen von Malware, Täuschungsversuchen und erpresserischen Ransomware-Attacken bis hin zu ausgeklügelten „Man-in-the Middle"-Angriffen, bei denen unternehmensinterne Kommunikationskanäle belauscht werden. Jeder dieser Angriffe kann erhebliche finanzielle Verluste verursachen, den Ruf eines Unternehmens schädigen und rechtliche Konsequenzen nach sich ziehen. Das Herstellen einer ausreichenden Resilienz ist deshalb für jedes Unternehmen wichtig.

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) jährlich einen umfassenden Überblick über die Bedrohungen im Cyberraum. Im Bericht für das Jahr 2023 kommt die Cybersicherheitsbehörde des Bundes zum Fazit: Die Bedrohung im Cyberraum ist so hoch wie nie zuvor.

Zunehmend stehen nicht nur große, zahlungskräftige Unternehmen, sondern auch kleine und mittlere Firmen im Fadenkreuz der Angreifer. Insbesondere bei den erpresserischen Ransomware-Attacken, die durch Verschlüsselung die Daten und IT-Systeme der angegriffenen Unternehmen unbrauchbar macht, verzeichnet das BSI eine im Vergleich zum Vorjahr stark erhöhte Aktivität.

Um die Systeme und Daten nach einem Ransomware-Angriff wieder zu entschlüsseln, verlangen die Cyberkriminellen in der Regel ein hohes Lösegeld, das sich am Unternehmenswert des jeweiligen Opfers orientiert. Um den Druck weiter zu erhöhen, wird ein zweiter Angriffsvektor immer beliebter. Die Kriminellen haben sensible

Unternehmensdaten in ihren Besitz gebracht und drohen mit der Veröffentlichung des gestohlenen Materials.

Das BSI gibt drei Ratschläge, um Verlusten und Schäden vorzubeugen:

- Unternehmen sollten ihre Resilienzen im Bereich IT-Security und Business Continuity so schnell wie möglich erhöhen, um Angriffen vorzubeugen und auf diese vorbereitet zu sein.

- Die Cybersicherheit muss aktiv gestaltet werden, um „vor die Welle" zu kommen.

- Generell gilt es, die Digitalisierung voranzubringen. Denn nur so werden deutsche Unternehmen auch in den Zukunftstechnologien sicher und wettbewerbsfähig. Dazu gehören Technologien wie Künstliche Intelligenz (KI), die Cloud, eID (elektronischer Online-Ausweis) und Smart Metering.

Der „Grüne Wiese"-Ansatz – klingt gut, ist aber zeitaufwändig und teuer

Angenommen, Cyberkriminelle waren mit ihrem Angriff erfolgreich, sind in die IT-Netze eines Unternehmens eingedrungen und haben einen Großteil oder im schlimmsten Fall alle Systeme vom Enterprise Resource Planning (ERP) bis zur Lagerverwaltung und den Kassensystemen am Point of Sale lahmgelegt. Der gewohnte Geschäftsbetrieb kommt zum Erliegen und die Priorität des Managements und der Geschäftsleitung liegt darauf, zumindest alle die zeitkritischen Geschäftsprozesse so schnell wie möglich wieder zum Laufen zu bringen.

Der Ansatz, die komplette IT inklusive aller Netzwerke und Desktoprechner, Laptops, Switches und Router neu aufzusetzen, liegt zunächst einmal nahe. Diese Methode, wie auf einer grünen Wiese die gesamte IT neu zu gestalten, ist auf den ersten Blick naheliegend. Sie ist aber auch sehr zeitaufwendig und zudem extrem kostenintensiv. Der Aufwand und vor allem die Komplexität, das wissen wir aus unserer Erfahrung als Breach Coaches und Sicherheitsberater, wird von den betroffenen Unternehmen in der Regel deutlich unterschätzt.

Ein Rechenbeispiel aus der Praxis verdeutlicht dies: Bei einem erfolgreich angegriffenen Unternehmen waren insgesamt 700 Server und etwa 7.000 Desktop-PCs und Laptops betroffen. Unter der sehr optimistischen Annahme, dass die komplette Neueinrichtung pro Rechner und Server etwa eine Stunde in Anspruch nimmt, betrüge der Zeitaufwand für den „Grüne Wiese"-Ansatz 7.700 Stunden, also über den Daumen etwa 3 ½ bis vier Mannjahre. Eins ist sicher: Auf diese Art und Weise kommen umsatzrelevante Geschäftsprozesse nicht schnell genug wieder in den produktiven Einsatz.

Die bessere, schnellere und sichere Alternative: Absicherung der Bestandssysteme

Schneller, besser und sicherer gelingt der Neustart nach einem erfolgten Cyberangriff durch die Absicherung der bestehenden Systeme und deren Weiternutzung. Als Breach Coaches und Sicherheitsberater, die in Krisensituationen zu Hilfe geholt werden, haben wir diese Methode bereits viele Male erfolgreich umgesetzt. Incident-Response-Dienstleister, die mit dieser Lösung vertraut sind, haben sich auch unter härtesten Bedingungen bewährt.

Ein solcher Incident-Response- oder auch Advanced-Persistent-Thread-Dienstleister - reinigt das bestehende IT-System, reagiert sofort auf Malware oder weitere Angriffsvektoren, die sich eventuell noch im System befinden und macht sie unschädlich. Es müssen also nicht – möglicherweise ebenfalls infizierte – Backups wiederhergestellt und die gesamte IT-Architektur inklusive Infrastruktur und weiterer Komponenten neu geplant und bereitgestellt werden. Es werden nur die Systeme neu aufgebaut oder „restored", die vom Angreifer komplett zerstört wurden. Vor allem Clients sind von einer Verschlüsselung häufig nicht oder nur teilweise betroffen. Spart man sich also die Neuinstallation in unserem oben genannten Rechenbeispiel, ist der Zeitvorteil enorm.

Eines unserer Kundenunternehmen hat einen Monat nach dem erfolgten Cyberangriff bereits einen neuen Produktionsrekord realisieren können. Mit dem „Grüne Wiese"-Ansatz sind derartige Erfolge wegen des immens erhöhten Zeit- und Kostenaufwandes außerhalb des Erreichbaren und Möglichen.

Leider erleben wir in der Praxis häufig, dass nach einer Ransomware-Attacke emotional beeinflusste Entscheidungen getroffen werden. Der Neuaufbau klingt so logisch wie zwingend, um einen sicheren Wiederanlauf zu gewährleisten. Ganz am Rande bemerkt sind die Berater, die diesen dringend empfehlen, häufig auch die Profiteure dieser Vorgehensweise, können sie sich doch für Wochen und Monate einer großen Menge Arbeit sicher sein.

Wir empfehlen daher dringend, sich über die Entwicklungen zu informieren. Erfolge, wie der oben beschriebene Fall, werden nicht zufällig erreicht. Sie werden möglich, wenn Unternehmen sich im Krisenfall von erfahrenen Beratern unterstützen lassen, die im besten Kundeninteresse und unter Einsatz der aktuellen technischen Möglichkeiten die Optionen aufzeigen, Risiken kalkulierbar machen und so einen sicheren und schnellen Wiederanlauf des Geschäftsbetriebes ermöglichen.

Die Empfehlungen des BSI und führender Analystenhäuser

Incident-Response-Dienstleister – auch APT-Response-Anbieter – stellen schneller ein hohes Maß an Sicherheit her, minimieren dadurch Umsatzverluste und schützen Unternehmen auch in Zukunft vor Cyberbedrohungen. Um die Transparenz am Markt zu erhöhen und Unternehmen die Anbieterauswahl zu erleichtern, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) APT-Anbieter auf Herz und Nieren geprüft.

Das gründliche Evaluationsverfahren gliederte sich in zwei Phasen:

1. **Überprüfung der vom Dienstleister bereitgestellten Dokumentation**
   Der Dienstleister musste zunächst eine vollständige Dokumentation bereitstellen. Hierzu zählten sowohl Beschreibungen der Produkte und Dienstleistungen als auch Erläuterungen in Bezug auf die Einhaltung der vom BSI aufgestellten Kriterien. Des Weiteren bestand die Möglichkeit, vorhandene Zertifizierungen von Rechenzentren oder dem Unternehmen selbst mitzuliefern.

Quelle: The Forrester Wave: Managed Detection and Response 2023

2. Durchführung eines Fachinterviews
In einem mehrstündigen Termin beim BSI musste der Dienstleister anhand fiktiver Szenarien zeigen, dass er in der Lage ist, die Situationen fach- und zielgerichtet zu bedienen. Dabei wurde sowohl auf das allgemeine Vorgehen des Dienstleisters als auch auf gestellte Fragen und Verarbeitung der erhaltenen Informationen geachtet.

Eine komplette Liste aller vom BSI evaluierter und als besonders zuverlässig ausgezeichneter APT-Response-Dienstleister finden Interessenten auf der Web-Präsenz des BSI. CrowdStrike (Nasdaq: CRWD), mit dem valantic eng zusammenarbeitet, ist einer dieser vom BSI qualifizierten APT-Response-Dienstleister.

CrowdStrike wurde von führenden Analystenhäusern wie Gartner und Forrester als Leader im Bereich Managed Detection and Response Services ausgezeichnet. Forrester schreibt in seinem „Managed Detection and Response (MDR)"-Report 2023 über CrowdStrike:

„CrowdStrike verbindet Produkte, Plattformen und Dienstleistungen nahtlos für seine Kunden. Nur wenige Unternehmen können eine solche Erfolgsserie vorweisen wie CrowdStrike. Der Dienstleistungsanbieter wurde zu einem herausragenden Incident-Response-Unternehmen und zu einem dominanten Akteur im Bereich der Endpunktsicherheit. CrowdStrike bietet einen außergewöhnlichen MDR-Service und hat Cybersecurity-Firmen gezeigt, wie Software-as-a-Service (SaaS)-Unternehmen funktionieren. CrowdStrikes umfassender Überblick über die Bedrohungslandschaft und die Incident-Response-Services verschaffen dem Unternehmen einen Vorteil, wenn es um Threat Intelligence und Managed Detection geht."

Darknet Monitoring – den Cyberkriminellen einen Schritt voraus sein

Wie bereits erwähnt: Die beste Antwort auf Cyberattacken besteht darin, es gar nicht erst zu einem erfolgreichen Angriff kommen zu lassen. Darknet Monitoring bietet die Möglichkeit, Attacken bereits in der Vorbereitungsphase zu erkennen bevor ein größerer Schaden entstehen kann und den Cyberkriminellen somit einen Schritt voraus zu sein.

Kurz zum Hintergrund des Cybercrime: Gehandelt werden gestohlenen und oft vertraulichen Daten, Logins, PINs, Passwörter, Identitäten oder Mailzugänge im Darknet, dem unsichtbaren, nicht ohne Weiteres zugänglichen Teil des World Wide Web. Cyberkriminalität ist heute hochprofessionell organisiert; unter den Hackern haben sich deshalb arbeitsteilige „Berufsgruppen" herausgebildet. Besonders spannend sind die Initial Access Broker, sozusagen die Immobilienmakler des Darknets. Sie bieten die ergaunerten Zugänge in Darknet-Foren, ähnlich wie auf einem eBay-Marktplatz, zum Verkauf an. Der Käufer, also der eigentliche Cyberangreifer, nutzt die gekauften Zugänge für den eigentlichen Angriff, um zum Beispiel IT-Systeme zu verschlüsseln und Lösegeld zu fordern.

Praxisbeispiel Versicherung: Cyberangriff vereitelt

Unsere Sicherheitsexperten sind im Zuge ihrer Recherchen im Darknet auf die Zugangsdaten einer großen deutschen Versicherung gestoßen, die auf einem der Marktplätze zum Verkauf angeboten wurden. Natürlich haben die Sicherheitsspezialisten den „Fund" unverzüglich der Versicherung gemeldet. Zwischen dem Verkauf der Daten und dem Angriff vergeht in der Regel einige Zeit. Das Unternehmen konnte dadurch rechtzeitig Schutzmaßnahmen einleiten und den Angriff vereiteln.

Solche, durch Darknet Monitoring mithilfe modernster Technologie recherchierte Informationen, sind Gold wert. Sie helfen, Schäden in Millionenhöhe zu verhindern.

Fazit & Beratung

Als erfahrene Cybersecurity-Berater versetzen wir die Geschäftsleitung, das Management und die IT-Leitung in die Lage, begründet eigenständige Entscheidungen zu fällen. Früher schon an später denken: Die Entscheidung, was im Notfall am besten zu tun ist, sollten Unternehmen im Vorfeld treffen. Dabei helfen sowohl eine Business-Impact-Analyse zur Bewertung der Geschäftsprozesse wie auch ein auf ihr Unternehmen abgestimmtes Risikoprofil, das Schwachstellen erkennt und absichert. Wir unterstützen Sie gerne mit unserer langjährigen Expertise und der Erfahrung aus Dutzenden erfolgreich durchgeführten Cybersecurity-Projekten.

Thomas Lang ist Partner und Managing Director der valantic Management Conuslting GmbH. Vor valantic hat er mehrere Unternehmen in der Dienstleistungsbranche gegründet und mehr als 20 Jahre IT-Erfahrung gesammelt, davon 15 Jahre in der Beratung.

Thomas Lang
Partner & Managing Director
+49 6103 5086-0
thomas.lang@mc.valantic.com
www.valantic.com

valantic Management Consulting GmbH
Dreieich Plaza 2A
63303 Dreieich
Deutschland

Telefon +49 6103 5086 0
info@mc.valantic.com

www.valantic.com

Stand April 2025