03 | 25 Sonderdruck für WatchGuard Technologies

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

Anwenderbericht:

WatchGuard-MDR bei der TERTIA Berufsförderung

www.it-administrator.de

Anwenderbericht: WatchGuard-MDR bei der TERTIA Berufsförderung

Rund um die Uhr

von Rebecca Horn

Es ist nicht die Frage, ob es ein Unternehmen trifft, sondern nur wann und wie schnell man dann reagieren kann – mit diesem Bewusstsein für die gegenwärtige Cyberbedrohungslage hat die TERTIA Berufsförderung bei der Absicherung der Endgeräte nachgerüstet. Seit März 2024 greift das Unternehmen auf das Security Operations Center von WatchGuard zurück. Dadurch erhält der Bildungsträger eine Rund-um-die-Uhr-Überwachung aller Endpunkte.

Das Thema IT-Security genießt bei der TERTIA Berufsförderung GmbH & Co. KG hohe Priorität. Neben der Absicherung der Zentrale in Alfter bei Bonn sowie den rund 150 deutschlandweiten Niederlassungen nimmt auch der Schutz von Homeoffice-Umgebungen eine entscheidende Rolle ein. Entsprechend hat das IT-seitig zentral organisierte Unternehmen in den letzten Jahren einen umfassenden Maßnahmenkatalog entwickelt, um so wenig Angriffsfläche wie möglich zu bieten.

Neben Netzwerkschutz und dem Wirken einer feingliedrigen Zugriffsverwaltung wird dem Bereich Endpoint-Security besondere Aufmerksamkeit entgegengebracht. Hier wurde in der Vergangenheit verstärkt investiert, wie Marcel Mörchen, einer der beiden IT-Leiter bei TERTIA, berichtet: "Man ist immer ein potenzielles Opfer. Inzwischen werden Hacker – wie es UN-Erkenntnisse beispielsweise im Fall Nordkorea belegen – schon von Regierungsseite angeheuert, um mit ihren kriminellen Machenschaften den Staatshaushalt aufzupäppeln. Vor solchen Entwicklungen dürfen wir nicht die Augen verschließen."

Bei TERTIA haben die IT-Verantwortlichen vor allem die von Ransomware ausgehende Bedrohung im Blick. Im Gegensatz zu anderen Organisationen sei das Unternehmen laut Mörchen für Angreifer wahrscheinlich weniger interessant, wenn es um den Diebstahl geistigen Eigentums geht. Aber allein das Verschlüsseln von Daten und Arbeitsumgebungen birgt in seinen Augen ein kaum zu unterschätzendes Verlustrisiko.

Einschläge im Umfeld nehmen zu

Etliche Firmen, mit denen TERTIA zusammenarbeitet, haben damit bereits einschlägige Erfahrungen gemacht und zusätzliches Wasser auf die Mühlen des Bildungsträgers gegossen, der insgesamt rund 1200 Mitarbeiterinnen und Mitarbeiter beschäftigt – davon fast die Hälfte mit Homeoffice-Option.

"Aus den persönlichen Erzählungen wissen wir bestens, wie groß der Schaden sein kann: Ein mehrwöchiger Totalausfall des IT-Systems und damit einhergehende aufwendige Wiederherstellungsarbeiten sind wohl ein Horrorszenario für jede IT-Abteilung." Die Gegenrechnung schafft dann ganz schnell ein konkretes Bewusstsein, wie Frederic Nowak, der von 2008 bis 2021 die IT-Strukturen im Team von TERTIA mitgestaltet hat und dem Unternehmen nun als externer IT-Dienstleister zur Seite steht, unterstreicht: "Wenn nur die Hälfte der Server verschlüsselt wird, können tausend Leute nicht arbeiten. Da braucht man kein Genie zusein, um zu wissen, wie viel Geld durch die Tür wandert." Entsprechend treffen die Hinweise des IT-Profis auf offene Ohren bei TERTIA – gerade wenn es um nachhaltige Absicherung geht.

Endpoint-Security als Paradedisziplin

Der Schutz der Endgeräte – von den Linux- und Windows-Servern über Desktop-PCs und Notebooks – spielt bei TERTIA eine wichtige Rolle. So haben die Verantwortlichen die Notwendigkeit professioneller Endpoint-Security bereits früh erkannt und seit den 1990er-Jahren kommen einschlägige Produkte zum Einsatz. Seit 14 Jahren vertraut das Unternehmen auf das Angebot von Panda Security/Cytomic, das im Zuge der 2020 erfolgten Akquise von Panda Security heute unter dem Dach von WatchGuard Technologies angesiedelt ist.

Insbesondere das Cloudfundament der Panda-Produkte fand beim Anbieter von Bildungsleistungen, der mittlerweile immer mehr Cloudanwendungen neben den physischen IT-Komponenten in seiner IT-Landschaft kombiniert, von Beginn an Anklang. "Über das Zusammenspiel von Cloudkonsole und den auf jedem Endgerät installierten Softwareagenten haben wir nicht nur umfassende Sicherheit gewon-

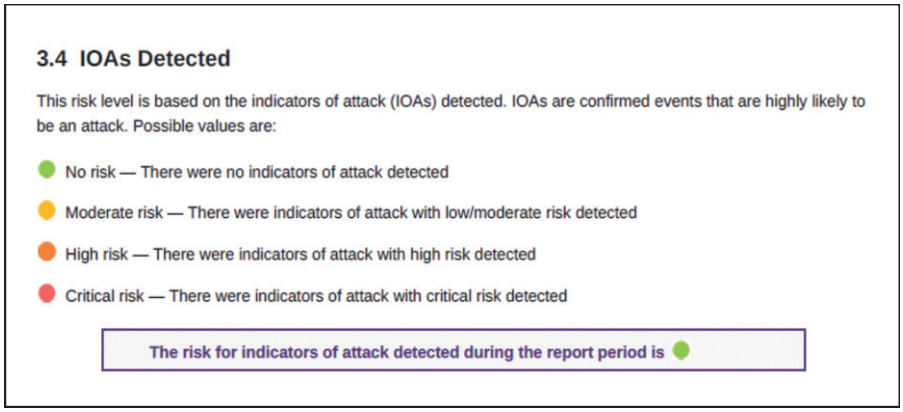
nen. Wir können alle relevanten Prozesse über eine zentrale Übersicht monitoren und einfach verwalten, ohne dafür selbst irgendwelche Kapazitäten für die dahinterstehende Technologie bereithalten zu müssen. In Sachen Preis-Leistung ist das Konzept für uns schon immer überzeugend gewesen", so Mörchen.

Mit der Gefahr mitgewachsen

Der Funktionsumfang wurde über die Jahre sukzessive ausgebaut. Von den intuitiven Möglichkeiten des Gerätemonitorings profitierte das IT-Team insbesondere nach Einführung des Patchmanagements. "Wir waren schon immer im Bilde, wenn es irgendwo einen Vorfall gab und konnten unternehmensübergreifend genau nachvollziehen, welche Geräte mit einem PC verbunden sind und wie sich der Webtraffic konkret gestaltet. Mit dem Leistungsbaustein des Patchmanagements sehen wir zudem, wo es Aktualisierungsbedarf gibt. Notwendige Updates können zeitnah und zielgerichtet erfolgen", erklärt Mörchen. Die Einstellungen können jederzeit bedarfsgerecht verfeinert werden, um die Sicherheit weiter zu erhöhen. So gilt beispielsweise in der Regel der sogenannte Hardening-Mode, der ein Ausführen unbekannter oder nicht erlaubter Skripte auf den Endgeräten automatisch verhindert. Auf diese Weise konnten in der Vergangenheit einschlägige Verschlüsselungsversuche bereits mehrfach abgewendet werden.

Anhand der Auswertungen der Logdateien verfolgte das IT-Team nicht zuletzt die konsequente Zunahme der Angriffsversuche, gerade in den letzten Jahren. Daher wurde seit 2023 über weitere mögliche Ausbaustufen bei der Endpoint-Security nachgedacht – obwohl die bestehenden Sicherheitsmechanismen bisher stets ohne größere Vorfälle gegriffen hatten. Mörchen: "Nachdem unser System nachweislich immer häufiger attackiert wird, war uns schnell klar, dass wir uns nicht auf dem Status quo ausruhen dürfen und die Nase vorn behalten müssen."

Es reifte der Plan zur Einführung eines Security Operations Centers (SOC), das die Bedrohungslage rund um die Uhr überwacht. Mit dem frisch aus der Taufe gehobenen MDR-Angebot von WatchGuard



Das Ampelsystem im monatlichen Report lenkt das Augenmerk auf außergewöhnliche Vorfälle und einschlägige Risiken.

eröffnete sich TERTIA eine neue, attraktive Umsetzungsoption, wie der IT-Leiter verrät: "Die Notwendigkeit eines SOC lag für uns auf der Hand. Anfangs haben wir durchaus überlegt, ein solches selbst aufzubauen. Von der Idee sind wir angesichts der hohen Initialkosten für eine entsprechend leistungsfähige Lösungslandschaft inklusive nötigem Personalaufwand jedoch schnell abgekommen. Zumal es allein damit ja nicht getan ist. Bei der Abwehr ausgefeilter Bedrohungen ist Expertise ein entscheidendes Kriterium. Das WatchGuard-MDR-Modell fanden wir daher bereits bei der ersten Vorstellung spannend."

Reaktionsstärke hat überzeugt

Bevor WatchGuard MDR den Zuschlag erhielt, wurden einige alternative Angebote geprüft, wie Mörchen ergänzt: "Die Entscheidung für ein SOC-Konstrukt ist mit einem nicht unerheblichen finanziellen Aufwand verbunden, auch in der Managed-Service-Variante. Allein deshalb haben wir genau verglichen und die Auswahl mit Bedacht getroffen". Seiner Erfahrung nach fallen die Preise, die Umsetzungspartner aufrufen, sehr unterschiedlich aus. Auch hinsichtlich der Möglichkeiten im täglichen Betrieb ergibt eine Abwägung Sinn.

Für WatchGuard sprach laut Mörchen dabei nicht nur die einfache Implementierung, da auf allen Endgeräten bei TERTIA bereits die nötigen Softwareagenten vorhanden waren. Am Ende zählte vor allem die gute Erfahrung der letzten vierzehn Jahre: "Der Faktor Vertrauen nimmt bei der Umsetzung von Securitythemen einen hohen Stellenwert ein, gerade wenn es um die nötige Rechtevergabe zum Zugriff auf das IT-System geht. Wenn man einen Anbieter so lange kennt, wie es bei uns mit Panda beziehungsweise WatchGuard der Fall ist, ist das Grundgefühl schon ein ganz anderes. Mit dem Team stehen wir seit Jahren persönlich in Kontakt. Die Zusammenarbeit haben wir immer als positiv und konstruktiv erlebt, auch wenn es mal Probleme zu lösen gab". Darin sind sich Mörchen und Nowak einig.

Der offizielle Startschuss für den MDR-Service von WatchGuard fiel im März 2024, seitdem laufen die Prozesse reibungslos. Einen ersten Eindruck von der Reaktionsstärke des WatchGuard SOC konnte sich das Team bei TERTIA aber bereits in der Testphase verschaffen. Mörchen erinnert sich: "Eines Tages kam die Nachricht aus dem SOC, dass es im Hinblick auf IT-Bewegungen Auffälligkeiten gab. Die Ursache konnte zügig gefunden und behoben werden. Jedoch war es für uns absolut beachtlich, wie schnell der Hinweis uns erreichte und in welcher Detailtiefe die Scans erfolgen. Es beruhigt schon ungemein, wenn man weiß, dass Profis alles im Blick haben und es im Fall der Fälle keine unnötigen Verzögerungen gibt."

Die Logdaten der insgesamt 4300 Endgeräte von TERTIA, die das SOC überwacht, sind über das eigene Managementsystem von Marcel Mörchen und seiner Mannschaft einsehbar: "Aber von uns sitzt eben keiner rund um die Uhr davor, um diese Daten auf eventuelle Anomalien zu durchleuchten, von den fehlenden technischen Möglichkeiten zur Auswertung ganz abgesehen. Da hat ein professionelles Security Operations Center ganz andere

Schlagkraft und erkennt selbst Kleinigkeiten, die uns möglicherweise nie aufgefallen wären."

Sofortige Aktion bei akuter Bedrohung

Um im absoluten Notfallszenario keine Zeit zu verlieren, sind die WatchGuard-Security-Experten von TERTIA bevollmächtigt, verdächtige Clients direkt vom Netz zu nehmen und zu isolieren, um einer möglichen Ausweitung des Angriffs im Netzwerk vorzubeugen. Parallel dazu erfolgt die Rücksprache mit Frederic Nowak im Hinblick auf weitere Schritte. "Für mich und TERTIA hat das sofortige Abschalten infizierter Geräte oberste Priorität. Abwarten und damit gegebenenfalls in Kauf nehmen, dass die Verseuchung weiter voranschreitet, ist keine Option. Von einem isolierten, einzelnen Endgerät geht keine Gefahr aus und wir gewinnen wertvolle Zeit, um uns ein Bild von der Lage zu machen. Wenn ein Mitarbeiter kurzfristig nicht arbeiten kann, ist das was ganz anderes, als wenn die gesamte Firma zum Erliegen kommt, weil man zu lange gezögert hat", so die Einschätzung von Frederic Nowak.

Von Vorteil ist, dass sich Endgeräte, die besonderer Aufmerksamkeit bedürfen, gezielt priorisieren lassen. Nowak dazu: "Von 4300 Endgeräten sind 4000 für das Funktionieren des unternehmensweiten Geschäfts wohl komplett irrelevant. Ein einzelnes Notebook ist schnell vom Netz genommen, deutlich prekärer ist die Lage bei Servern." Auf diesen liegt daher ein gesonderter Fokus. Auf Basis der granularen Informationen des SOC lassen sich Abwehrmaßnahmen passgenau, verlässlich und minimalinvasiv steuern – im Einklang mit der IT-Security-Gesamtstrategie.

Der Mehrwert zeigt sich aber auch jenseits von Ausnahmesituationen, die es bei TERTIA bisher zum Glück noch nicht gab. Das Reporting des SOC trägt zu normalen Arbeitszeiten ebenfalls zur Entlastung der internen IT-Abteilung bei. Regelmäßig geben detaillierte Berichte über ein Ampelsystem leicht nachvollziehbar Auskunft zum Status quo der Schutzvorkehrungen und machen beispielsweise darauf aufmerksam, wenn ein Dienst keine Rückmeldung gibt oder Aktualisierungsbedarf bei den Clients besteht. So kann das IT-Team strukturiert prüfen und auf Endpoints erkannte Lücken konsequent schließen. "Für uns geht das Konzept auf. Mit den Experten von WatchGuard im Rücken sehen wir uns bestens aufgestellt. Meldungen über neue, erfolgreiche Angriffsversuche, die Unternehmen weltweit in Atem halten, nehmen wir inzwischen weitaus entspannter zur Kenntnis", so Marcel Mörchen abschließend.

Über die TERTIA Berufsförderung

Die 1973 gegründete TERTIA Berufsförderung GmbH & Co. KG gehört deutschlandweit zu den größten Anbietern im Bereich Erwachsenenbildung und Berufsförderung. Mit insgesamt rund 1200 Mitarbeitern sowie zahlreichen freien Dozenten unterstützt TERTIA – sowohl im Rahmen von Präsenzkursen an 150 Standorten in vierzehn Bundesländern als auch über einen Online-Campus – Menschen mit unterschiedlichsten Qualifikationen bei der beruflichen Weiterentwicklung.

Das Angebot des bei Arbeitsagenturen, Jobcentern und Kommunen etablierten Bildungsträgers und IHK-Partners reicht von Maßnahmen zur Wiedereingliederung und Begleitung von Langzeitarbeitslosen über Umschulungen, Coachings und Sprachkurse bis hin zu klassischen Berufsausbildungen. Der Stammsitz des Familienunternehmens, das nicht zuletzt interessierten Privatpersonen Qualifizierung und Weiterbildung ermöglicht und Firmen auf Wunsch bei der Fachkräftesuche zur Seite steht, ist in Alfter bei Bonn.

Fazit

Die Einführung des Managed Detection and Response (MDR)-Angebots von WatchGuard bei der TERTIA Berufsförderung unterstreicht, wie entscheidend eine proaktive und professionelle Absicherung von Endgeräten angesichts der heutigen Bedrohungslage ist. Durch die Rund-um-die-Uhr-Überwachung und das gezielte Eingreifen bei Auffälligkeiten gewinnt das Unternehmen nicht nur an Sicherheit, sondern entlastet auch die interne IT-Abteilung. Besonders beeindruckend ist, wie sich jahrzehntelange Erfahrung mit Endpoint Security in einer kontinuierlichen Optimierung der Schutzmaßnahmen niederschlägt, die den wachsenden Anforderungen standhalten.

Das Beispiel von TERTIA zeigt, dass IT-Security nicht als statisches Konzept, sondern als dynamischer, mitwachsender Prozess verstanden werden muss. Mit der Entscheidung für ein externes SOC wird deutlich, dass nicht nur technologische Lösungen, sondern auch Vertrauen und langjährige Partnerschaften eine entscheidende Rolle spielen. Unternehmen, die wie TERTIA rechtzeitig auf diese Schlüsselfaktoren setzen, können Angriffen mit Gelassenheit begegnen und ihre Widerstandsfähigkeit nachhaltig stärken. *(dr)* IT

Rebecca Horn ist PR-Redakteurin bei Press'n'Relations mit den Schwerpunkten IT und Energie.