PKN Kundenreferenz
World Wildlife Fund for Nature

Sicher in die Zukunft:
Wie der WWF Deutschland seine digitale Umwelt zeitgemäß schützt

„Unsere Erwartungen sind hundertprozentig erfüllt worden. Wir fühlen uns mit der Lösung von Arctic Wolf wohl und vor allem sicher. Nicht zuletzt, weil wir auf der anderen Seite hochkompetente Menschen haben, mit denen wir kommunizieren können."

Stefan Brülle,
Chief Information Security Officer (CISO)
beim WWF Deutschland

Der WWF stand vor der Herausforderung, ein nicht mehr zeitgemäßes IT-Sicherheitssystem ohne zentrale Plattform für Logfile-Analyse oder effektives Alerting und ohne die Möglichkeit eines 24/7-Supports zu modernisieren und um spezialisierte IT-Sicherheitsexpertise zu ergänzen. Mit der PKN und deren Empfehlung, Arctic Wolf, fand der WWF die benötigte umfassende IT-Sicherheitslösung, die nicht nur kostengünstiger als erwartet war, sondern auch hochkompetente Ansprechpartner für direkte Kommunikation und schnelle Reaktionszeiten auf Sicherheitsbedrohungen bot. Die Partnerschaft verbesserte signifikant die IT-Sicherheit und Arbeitsprozesse des WWF, ermöglichte präzise Alerts, persönlichen Austausch mit Experten und stellte eine proaktive Unterstützung bei potenziellen Incidents dar, was die Investition in Arctic Wolfs Cyber-Security-Lösung zu einer effektiven und kosteneffizienten Entscheidung für die spendenfinanzierte NGO machte.

PKN DER IT-MAßSCHNEIDER

ARCTIC WOLF

AUF EINEN BLICK

Land: weltweit
Branche: gemeinnützige Organisation

UNTERNEHMEN

Der WWF (World Life Fund for Nature) Deutschland, Teil einer weltweiten Bewegung, entstand 1963, zwei Jahre nach der Gründung des WWF International im Jahr 1961. Mit einem Startkapital von 85.000 DM hat sich der WWF zu einer führenden Organisation entwickelt, die über 13.000 Schutzprojekte in mehr als 150 Ländern mit rund 7,3 Milliarden Euro unterstützt hat.

HERAUSFORDERUNG

Der mit einem Dachverband und unterschiedlichen Landesorganisationen international agierende WWF Deutschland stand vor der Herausforderung, dass sein IT-Security-Konzept nicht mehr zeitgemäß war. Es fehlte es an ausreichendem Personal für einen 24/7 Support, das Know-how im Bereich SOC war aufgrund der Vielfältigkeit und Anzahl der Systeme und Schnittstellen unzureichend.

LÖSUNG

Der WWF nutzte die Dienstleistungen von Arctic Wolf. Dessen Angebot wurde u.a. mit 24/7 SOC-Dienstleistungen den IT-Sicherheitsanforderungen des WWF effektiv gerecht und überzeugte nicht zuletzt durch ein hervorragendes Preis-Leistungs-Verhältnis.

NUTZEN

Dank der Partnerschaft mit Arctic Wolf und der Implementierung eines zeitgemäßen IT-Security-Konzepts ist der WWF nun deutlich besser vor externen Cyber-Angriffen geschützt und verfügt über eine robuste, zeitgemäße Sicherheitsinfrastruktur.

Weltweit aktiv für Umweltschutz und Artenvielfalt

Der WWF (World Wildlife Fund for Nature), gegründet im Jahr 1961, ist eine der führenden unabhängigen Naturschutzorganisationen der Welt, die sich dem Erhalt der biologischen Vielfalt und der Reduzierung schädlichen Einflussfaktoren der Menschheit auf die Umwelt widmet. Mit Projekten in über 100 Ländern verfolgt der WWF das Ziel, die weltweit wichtigsten ökologischen Regionen zu schützen, die Verschmutzung und den übermäßigen Konsum natürlicher Ressourcen zu reduzieren und nachhaltige Ansätze für die Nutzung der natürlichen Ressourcen zu fördern.
Der WWF Deutschland engagiert sich stark im Schutz der Natur und bedrohter Arten sowie im Kampf gegen den Klimawandel. Zu seinen Hauptinitiativen gehören der Erhalt biologischer Vielfalt, der Schutz von Wäldern, Ozeanen und Süßwasserökosystemen, die Reduzierung von Treibhausgasemissionen, die Förderung nachhaltiger Landwirtschaft und Fischerei sowie spezifische Projekte zum Schutz heimischer Arten und Lebensräume in Deutschland.

Überwindung von IT-Sicherheitsherausforderungen: Der Weg zur Modernisierung

Die Herausforderungen, mit denen der WWF konfrontiert war, spiegelten die komplexen Anforderungen an eine moderne IT-Sicherheitsinfrastruktur wider.
Bis Anfang 2023 war keine zentrale Plattform vorhanden, auf der alle Logfiles gesammelt und analysiert werden konnten. Dieses Fehlen eines zentralisierten Logfile-Systems verhinderte eine effektive Überwachung und Analyse von Sicherheitsereignissen. Zudem gab es kein zentrales Alerting-System; lediglich Alarmmeldungen von der Firewall, und die Standardverfahren der Microsoft 365 Umgebung, standen zur Verfügung, ohne dass diese Meldungen konsistent in das Ticketsystem des WWF eingespeist werden konnten.
Angesichts begrenzter Ressourcen war es dem WWF nicht möglich, einen kontinuierlichen 24/7-Support zu gewährleisten. Außerhalb der regulären Geschäftszeiten, an Wochenenden und Feiertagen, fehlte eine IT-Sicherheitsbereitschaft gänzlich. Zusätzlich fehlte eine spezialisierte Expertise in IT-Sicherheitsthemen, ebenso wie ein Partner für das Incident Response Management.
Trotz dieser Ausgangslage hatte der WWF bis dahin glücklicherweise keine schwerwiegenden Cyber-Sicherheitsvorfälle zu verzeichnen. Jedoch war die Organisation angesichts der zunehmenden Zahl von Cyberangriffen auf Kommunen, Kliniken, Universitäten und andere Institutionen alarmiert. Besonders als eine NGO, die oft im Fokus der Öffentlichkeit steht, war sich der WWF des Risikos bewusst, leicht zum Ziel von Cyberangriffen zu werden. Die Notwendigkeit gerade für eine spendenfinanzierte Organisation, präventive und strategische Maßnahmen zu ergreifen, um schwerwiegende Sicherheitsvorfälle und damit existenzgefährdende wirtschaftliche Schäden oder einen nicht wieder gut zu machenden Imageverlust zu verhindern, war offensichtlich.
Für die anspruchsvolle Zielsetzung, insbesondere ein umfassendes Alerting und eine effektive Logfile-Analyse, reichten die internen Ressourcen nicht aus. Daher entschied sich der WWF, nach einem externen Partner für IT-Sicherheit zu suchen, und führte zunächst eine Bestandsaufnahme durch, um die bestehenden Sicherheitslücken genau zu identifizieren.

Wie der WWF seine IT-Sicherheit zeitgemäß aufstellte

Gezielte Recherchen führte den WWF zur PKN. Die PKN wiederum empfahl Arctic Wolf als idealen Partner für das Vorhaben, da der WWF eine umfassende IT-Sicherheitslösung aus einer Hand suchte.

Im Frühjahr 2023 lud der WWF PKN und Arctic Wolf zur Teilnahme an der Ausschreibung ein. Dank des überzeugendsten Konzepts erhielten sie den Zuschlag für das Projekt. Ausschlaggebend war u.a. der Service von Arctic Wolf, der die ständige Verfügbarkeit von persönlichen Ansprechpartnern einschloss. Zudem waren die Kosten für die Dienstleistungen von Arctic Wolf günstiger als ursprünglich vom WWF kalkuliert, was die Entscheidung zusätzlich erleichterte.

Zum Paket gehören:

I. MANAGED DETECTION & RESPONSE

24x7 Managed Detection & Response/ Netzwerk-Monitoring
Zugewiesenes Concierge Security Team (CST), Security Engineer & Analyst
Erweiterung des eigenen Security-Teams durch das CST
Umlimitierte Anfragen und Zugriff auf das CST und das 24x7 iSOC
Regelmäßige strategische Meetings mit dem CST zur Verbesserung der IT-Sicherheit des Unternehmens
Unlimitierte Benutzung des Agenten
Isolierung der Endgeräte durch den Agenten
Reporting für die IT-Abteilung und das Management: Ad hoc, wöchentlich, monatliche, quartalsweise
Kundenspezifische Reportings auf Anfrage
Unlimitiertes Log und Datenvolumen
Unlimitierte Events pro Sekunde
90 Tage Aufbewahrung aller Logs
Unlimitierte Anzahl von kundenspezifischen Erkennungsregeln (Custom-Rules)
Überwachung des gesamten Internetverkehrs durch den Sensor (IDS, IPS, flow data)
Monatliche External Vulnerability Assessments inkl. Web Applikationen
Darknet-Scanning mit Account-Takeover-Prävention
Incident Response Retainer

II. MANAGED RISK

Zugewiesenes Concierge Security Team (CST), Security Engineer und Analyst
Kontinuierliche und Host-basierte Vulnerability Assessments
Asset Identifizierung und -Klassifizierung
Risikoprofil-Erstellung und Empfehlungen
Regelmäßige Überprüfung der Risikoposition mit dem CST
CIS Benchmarking
Alarmierung bei kritischen Sicherheitslücken
Wöchentliche external Vulnerability Assessments inkl. Web-Applikationen

PKN Kundenreferenz
World Wildlife Fund for nature

Lernkurven und Erfolge der IT-Sicherheitswende

Die Partnerschaft mit PKN und Arctic Wolf erwies sich als sehr erfolgreich.
Gleichwohl gab es Rückmeldungen, die auf Verbesserungspotenziale hinwiesen. Stefan Brülle, CISO beim WWF Deutschland, merkte selbstkritisch an, dass der WWF sich rückblickend noch intensiver über die mit dem Projekt verbundenen Anforderungen hätte informieren sollen. Gleichzeitig wurde der Wunsch geäußert, dass Arctic Wolf den Aufwand für das Onboarding klarer und realistischer hätte kommunizieren sollen, da der tatsächliche Zeitaufwand einschließlich Feinabstimmung näher an drei Monaten als an den ursprünglich angenommenen drei Wochen lag. Eine transparentere Kommunikation vor Projektbeginn, insbesondere über die benötigten Ressourcen und die zu erledigenden Aufgaben, wäre also hilfreich gewesen.
Die Zusammenarbeit mit PKN wurde ebenfalls sehr geschätzt, wobei der persönliche und lösungsorientierte Ansatz des Ansprechpartners Günter Nikel hervorgehoben wurde. Die Unternehmensgröße von PKN ermögliche nach den Erfahrungen des WWF einen persönlichen Kontakt auch überhaupt erst; bei sehr großen IT-Unternehmen sei dies sehr viel schwieriger. Der WWF fühlte sich bei PKN gut aufgehoben, da die versprochene Qualität der Dienstleistung stets erfüllt und gehalten wurde. Einzig das Fehlen eines Verweises auf die AGB von Arctic Wolf im PKN-Angebot habe wegen einer deshalb durch den WWF separat zu leistenden Unterschrift zu einer unnötigen Verzögerung im Prozess geführt.
Insgesamt brachte die Partnerschaft mit PKN und Arctic Wolf dem WWF eine umfassende und effektive IT-Sicherheitslösung, die die Organisation deutlich besser vor Cyber-Bedrohungen schützt.

Nach der Transformation der IT-Sicherheit: Wie der WWF heute aufgestellt ist

Das Ergebnis und der Nutzen der Partnerschaft zwischen dem WWF und Arctic Wolf manifestiert sich in einer signifikanten Verbesserung der IT-Sicherheit und der Arbeitsprozesse innerhalb der Organisation. Durch die Implementierung der Cyber-Security-Lösung von Arctic Wolf erhält der WWF nun präzise Alerts, die eine schnelle Reaktion auf potenzielle Bedrohungen ermöglichen. Besonders wertvoll für den WWF ist der Zugang zu hochkompetenten Ansprechpartnern bei Arctic Wolf. Diese Experten stehen für Rückfragen zur Verfügung, bieten detaillierte Analysen und Empfehlungen an und unterstützen bei der Bewertung und Einordnung von Sicherheitsereignissen. Diese direkte und persönliche Kommunikationsmöglichkeit bietet dem WWF eine enorme Erleichterung im Arbeitsalltag.
Die Möglichkeit, jederzeit Tickets zu eröffnen und konkrete Fragen zu stellen, wird von den WWF-Mitarbeitern als besonders vorteilhaft empfunden. Antworten und Empfehlungen werden in der Regel innerhalb eines Tages geliefert, was die Reaktionsfähigkeit der Organisation im Falle von Sicherheitsvorfällen deutlich verbessert. Der persönliche und regelmäßige Austausch mit den Experten von Arctic Wolf hebt sich positiv vom vorherigen Zustand beim WWF ab und trägt dazu bei, Unsicherheiten effektiv zu bewältigen.
Obwohl der WWF bislang noch keinen größeren Incidents zu verzeichnen hatte, wurde die proaktive Unterstützung von Arctic Wolf bereits in einer frühen Phase der Partnerschaft unter Beweis gestellt. Bei einer Fehlfunktion in der Firewall, die einen Angriff vermuten ließ, bot Arctic Wolf unverzüglich und unkompliziert Hilfe an und integrierte sich aktiv in die Krisenbewältigung des WWF. Dieses Engagement, selbst vor dem offiziellen Onboarding, zeigte deutlich, dass Arctic Wolf ein verlässlicher Partner ist, der im Notfall schnell und unkompliziert Unterstützung bietet.
Zusammengefasst hat der WWF in Arctic Wolf einen Partner gefunden, der nicht nur durch technische Lösungen überzeugt, sondern auch durch menschliche Zugänglichkeit und eine partnerschaftliche Kommunikation. Diese Zusammenarbeit erfüllt die Erwartungen des WWF vollständig und wird als beispielhaft für andere Unternehmen empfohlen.
Natürlich stellt die Implementierung dieses umfassenden IT-Security-Konzepts gerade für eine spendenfinanzierte NGO wie den WWF ein Investment dar, das wohldurchdacht sein will. Heute ist der WWF überzeugt, dass die Investition in die Cyber-Security-Lösung von Arctic Wolf die kosteneffizienteste und wirksamste Strategie war, um die Organisation vor Cyber-Bedrohungen zu schützen und die IT-Sicherheit nachhaltig zu verbessern.

PKN
DER IT-MAßSCHNEIDER

ARCTIC WOLF