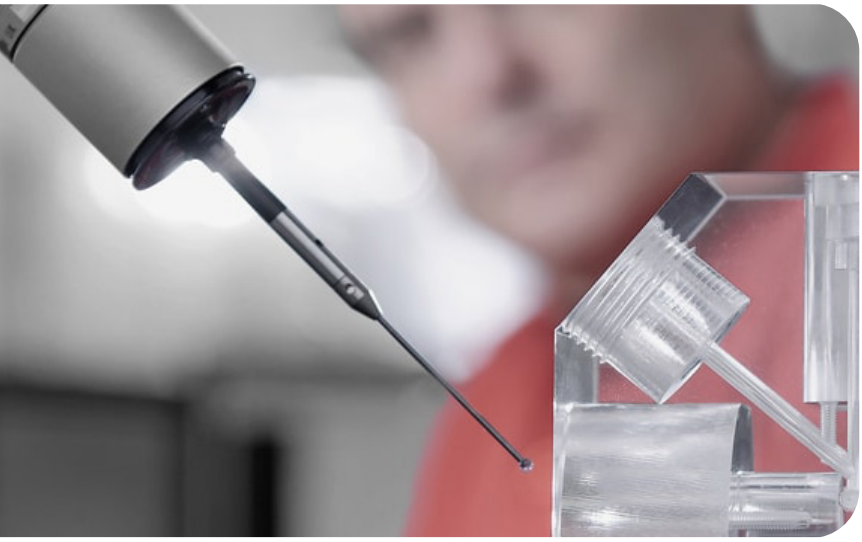
Ontinue

Referenzkunde

Ontinue schützt die schweizer BBC Group rund um die Uhr



Jeder Schweizer kommt jeden Tag durchschnittlich zwei Mal mit Produkten und Dienstleistungen der Behr Bircher Cellpack BBC AG in Kontakt. Das mittelständische Traditionsunternehmen wurde von Giorgio Behr offiziell im Jahr 2003 gegründet, die Wurzeln reichen allerdings bis in die frühen 1990er-Jahre zurück. Die Familie Behr, unter deren Führung die Behr Bircher Cellpack BBC AG bis heute steht, hat die Firmenbereiche sukzessive ausgebaut und immer wieder neue Geschäftsfelder erschlossen. So wurde über die Jahre aus dem Unternehmen die mittelständische BBC Group, die sich in sechs Teilbereiche untergliedert.

Heute ist die Unternehmensgruppe in den langfristig bedeutenden Märkten der Energieverteilung, Kunststoffbearbeitung, Medizintechnik und Verpackung, aber auch in den Bereichen Sicherheit und Komfort tätig. Diese Diversität führt dazu, dass die BBC Group auch als mittelständisches Unternehmen eine komplexe Standort- und Organisationsstruktur aufweist: Sie ist in vielen Ländern in Nord- und Südamerika, Europa und Asien vertreten. Durch die weitläufige Vernetzung der Standorte ist auch die Bedrohungslage durch Cyberattacken größer als das bei vergleichbaren Mittelständlern der Fall ist.

„Von unseren Partnern, Lieferanten und Kunden hören wir immer wieder, dass die Anzahl der Cyberattacken zunimmt", erklärt Thomas Stadler, CIO der BBC Group. „Wir können eine Verschärfung der Bedrohungslage ebenfalls feststellen, auch wenn unsere Sicherheitsmaßnahmen bislang glücklicherweise ausgereicht haben. Doch es ist nur eine Frage der Zeit, bis sie das nicht mehr tun.
"Es ist kein Wunder, dass kleine und mittelständische Unternehmen wie die BBC Group mehr und mehr in den Fokus von Hackern geraten: Da Konzerne in der Regel über höchste Sicherheitsmaßnahmen verfügen und ihre Systeme rund um die Uhr schützen können, richten Cyberkriminelle ihr Augenmerk daher auf vermeintlich leichtere Opfer.

BBC GROUP

Motivation

- Sicherheitsabdeckung rund um die Uhr
- Schnellere Reaktionszeit bei Angriffen
- Mehr Awareness für Cybersecurity im Unternehmen
- Bessere Nutzung vorhandener Sicherheitsinfrastruktur

Lösung

- Enge Zusammenarbeit mit externem SOC via Microsoft Teams
- Schaffung des Postens eines Security-Engineers für die Kollaboration mit dem MXDR-Dienstleister
- Threat Intelligence durch Ontinue ION

Ergebnis

- 24/7-SOC-Abdeckung
- Teilautomatisierung wichtiger Sicherheitsprozesse
- Reduzierung der MTTR und gefährlicher Phishing-Attacken
- Mehr Wertschöpfung aus vorhandenen Daten

Über die BBC Group

Die Behr Bircher Cellpack BBC Group ist in den langfristig bedeutenden Märkten der Energieverteilung, Kunststoffbearbeitung, Medizintechnik und Verpackung (BBC Cellpack) sowie Sicherheit und Komfort (BBC Bircher) tätig. Dank ihrer breiten internationalen Präsenz mit Fertigung und Vertrieb sind sie ein kompetenter und äußerst konkurrenzfähiger Partner.

„Man muss sich schützen, sonst ist man das schwächste Glied in der Kette“, betont Alex Oehler, Head of IT Infrastructure & Systems Management der BBC Group. „Hundertprozentige Sicherheit ist illusorisch, aber es muss das erklärte Ziel eines mittelständischen Unternehmens sein, den nötigen Aufwand für Hacker, einen erfolgreichen Cyberangriff durchzuführen, so hoch zu treiben, dass er sich nicht mehr lohnt.“

Dazu gehört eine möglichst wasserdichte Sicherheitsinfrastruktur, die bei der Behr Bircher Cellpack BBC AG in Form von Microsoft Sentinel und M365 Security softwareseitig bereits vorlag. Problematisch war bis dato allerdings die Betreuung der Warnungen rund um die Uhr und die Threat Intelligence – zwei wichtige Puzzleteile im Kampf gegen Cyberattacken, die nur ein Security Operations Center (SOC) gewährleisten kann.

Synergien sinnvoll nutzen

Personalmangel und enge Budgets erlauben es praktisch keinem Mittelständler, ein dediziertes SOC aufzubauen. Daher entschied sich die BBC Group, auf Outsourcing und den MXDR (Managed Extended Detection and Response)-Service ION von Ontinue zu setzen. Da die Unternehmensgruppe bereits bei der Implementierung ihres softwaredefinierten Netzwerks (SD-WAN) mit dem Team von Open Systems – aus der die Ontinue entsprungen ist – sehr erfolgreich zusammengearbeitet hat, war es nur logisch, beim SOC-Dienstleister auf Ontinue zu setzen. Auch Microsoft, deren Sicherheitsplattform die BBC Group nutzt, bekräftigte diese Entscheidung in der Evaluierungsphase mit einer Empfehlung.

Gleichzeitig schuf die Unternehmensgruppe intern die Position eines Security-Engineers, also des für externe SOC-Teams so wichtigen Insiders, der mit den Sicherheitsexperten des Dienstleisters zusammenarbeitet. Diese Schnittstelle zwischen der internen IT-Abteilung der BBC Group und dem SOC von Ontinue ist von immenser Bedeutung, denn externe Dienstleister haben niemals einen so tiefen Einblick in die Systeme wie unternehmenseigene Experten.

Die praktische Umsetzung all dieser Maßnahmen nahm nur etwa zwei Monate in Anspruch. Diese kurze Zeitspanne konnten die BBC Group und Ontinue einhalten, da die Sicherheitssoftware von Microsoft bereits solide konfiguriert war. Somit war es lediglich notwendig, den neuen Security Layer auf das funktionale Fundament zu heben.

Bessere MTTR durch rationalisierte Kollaboration

Praktisch verbessert und rationalisiert Ontinue ION die Kommunikation, indem der MXDR-Service das Ticketsystem sowie Warnmeldungen per E-Mail in einen schlanken und übersichtlichen Microsoft-Teams-Channel verlagert. Auf diese Weise versickern Warnungen nicht ungesehen in den überfüllten Postfächern der internen IT-Experten. In Verbindung mit der 24/7-Überwachung der IT-Infrastruktur konnte die BBC Group ihre Reaktionszeit bei Cyberattacken und ihre Mean Time To Respond (MTTR) deutlich verringern.

Durch seine Threat-Intelligence-Kapazitäten half Ontinue der Unternehmensgruppe, Schwachstellen aufzudecken. Wie die meisten Unternehmen hat die BBC Group erkannt, dass das individuelle Fehlverhalten von Nutzern eine persistentes und erhebliches Risiko darstellt, welches adressiert werden muss. Dieses Wissen führte zu Awareness-Kampagnen sowie halbautomatischen Sicherheitsprozessen, die in kürzester Zeit die Anzahl gefährlicher Phishing-Attacken um die Hälfte reduzierten. Klickt ein User heute beispielsweise auf einen verdächtigen Link, der eine Warnung auslöst, muss ein Mitglied des Security-Teams lediglich den Namen in das System eingeben. Schon wird der User automatisch ausgesperrt und erhält einen Sicherheitsschlüssel, mit dem er ein neues Passwort für seinen Account setzen und sich wieder einloggen kann.

Zukünftig möchte die BBC Group noch mehr in Security investieren und plant, die gute Zusammenarbeit mit Ontinue auszubauen. Gerade die Bereiche Threat Intelligence und Vulnerability-Management werden dabei eine große Rolle spielen: Ziel ist es, sukzessive Sicherheitslücken zu identifizieren und zu schließen. „Es ist ein Fakt, dass Security für die Anwender zumeist unbequem ist“, so Thomas Stadler, „jedoch ändert dies nichts an der unternehmerischen Notwendigkeit eines ausreichenden Sicherheitsdispositives und mit Ontinue haben wir einen Security-Partner an der Seite, der mich nachts gut schlafen lässt.“

„Das Thema Security ist für Anwender oft unbequem, unternehmerisch aber leider notwendig. Dank Ontinue schlafe ich nachts besser, da deren Experten uns rund um die Uhr schützen.“

Thomas Stadler
CIO
BBC Group

Ontinue

Über Ontinue

Ontinue, der Experte für KI-gestützte Managed Extended Detection and Response (MXDR), ist ein rund um die Uhr verfügbarer Sicherheitspartner mit Hauptsitz in Zürich. Um die IT-Umgebungen seiner Kunden durchgehend zu schützen, ihren Sicherheitsstatus zu bewerten und kontinuierlich zu verbessern, kombiniert Ontinue KI-gesteuerte Automatisierung und menschliches Fachwissen mit dem Microsoft Sicherheits Produktportfolio. Durch die intelligente, Cloud-basierte Nonstop SecOps Plattform reicht Ontinues Schutz vor Cyberattacken weit über die grundlegenden Detection und Response Services hinaus.

Weitere Informationen gibt es unter www.ontinue.com