CASE STUDY / RED BULL

Managed Security: So sieht eine Zusammenarbeit aus

Managed Security: That's how a good collaboration works

„Ein SOC als Managed Service dient als das zweite Sicherheitsnetz im Balanceakt IT-Sicherheit“

“A SOC as a managed service provides a second line of defence in the balancing act that is IT security”

— Jimmy Heschl, Head of Digital Security Red Bull

Bild/Image: istock.com/milanvirijevic

Der Energy Drink Red Bull ist weltweit bekannt. Aktivitäten im Automobilsport, Fußball und Eishockey, das Sponsoring von Athleten oder Projekte wie Red Bull Air Race tragen zur starken Marke bei. Auch verschiedene Medienunternehmen in den Bereichen Produktion, TV und Verlagswesen gehören zur Unternehmensgruppe. Alle Bereiche zusammen ergeben eine weltumfassende IT-Landschaft mit großen Datenmengen, laufenden Standorterweiterungen und Integrationen von neuen Unternehmen und Bereichen.

Im Bereich IT-Sicherheit nutzt Red Bull die Managed Services von RadarServices. Das kontinuierliche IT Security Monitoring und die Schwachstellenerkennung werden von RadarServices für alle IT-Standorte und Bereiche von Red Bull weltweit erbracht, sämtliche Daten werden integriert und die erkannten sicherheitsrelevanten Informationen tagesaktuell und zentral im dafür bereitgestellten Risk & Security Cockpit an die Sicherheitsverantwortlichen in die Zentrale berichtet.

Wie gestaltet sich die Zusammenarbeit mit dem Managed Services Provider in der Praxis? Jimmy Heschl, Head of Digital Security bei Red Bull, gibt einen Einblick.

Herr Heschl, wie ist das Thema IT Security in Ihrem Haus verankert?

Zwei grundlegende Gedanken sind für unser IT-Sicherheitsmanagement zentral: Einerseits denken unsere internen, operativen IT-Teams Sicherheit mit. Damit haben wir nicht das Problem, IT-Sicherheitsmaßnahmen „on top“ zu Veränderungen in unserer IT-Landschaft nachziehen zu müssen, sondern gehen sicherheitsseitig Hand in Hand und stehen im ständigen Dialog mit denen, die die IT operativ weltweit betreuen. Andererseits sind wir uns bewusst, dass die Sicherheit einer IT-Landschaft nicht durch Tech-

The Red Bull energy drink is famous throughout the world. Motorsport, football and ice hockey activities, the sponsoring of athletes or projects such as the Red Bull Air Race, all help to establish a strong brand. Miscellaneous media companies in production, TV and publishing are also part of the corporate group. Put them all together and a global IT landscape emerges with vast quantities of data, regular expansion of locations and the integration of new companies and sectors.

Red Bull uses the managed services of RadarServices for IT security. This service provider implements ongoing IT security monitoring and vulnerability detection for all Red Bull's IT locations and sectors worldwide. All the data is integrated and detected information relevant to security is reported in the RadarServices Risk & Security Cockpit on a daily basis to those responsible for security at the Red Bull headquarters.

How does the collaboration with the managed services provider work in practice? Jimmy Heschl, Head of Digital Security at Red Bull, offers an insight.

Mr Heschl, how do you incorporate the issue of IT security in your company?

Two basic concepts are fundamental to our IT security management. Firstly, security is enshrined in the thinking of our internal, operational IT teams. This means that we do not have the problem of needing to implement IT security measures “on top” of changes in our IT landscape, but we collaborate, from the security point of view, and are in constant dialogue with those who manage IT operationally worldwide. Secondly, we are aware that the security of an IT landscape cannot be achieved by technology alone. It would not work without the experts, their excellent handling of highly specialised software and our strong trust and confidence in their abilities.

nologie allein erzielt werden kann. Ohne Experten, die hervorragend mit hochspezialisierter Software umgehen können und in deren Fähigkeiten wir auch tatsächlich vertrauen können, geht es nicht.

Für die tägliche Überwachung der IT-Sicherheit greifen Sie schon seit Jahren auf die Managed Services von RadarServices zurück. Ihr internes IT Security Team arbeitet also täglich mit den Sicherheitsanalysten aus Europas größtem Security Operations Centre in Wien zusammen. Wie kann man sich diese Zusammenarbeit genau vorstellen?

Die KollegInnen von RadarServices geben uns alle erkannten sicherheitsrelevanten Probleme weiter, priorisieren und bewerten sie für uns. Auch Anleitungen, was zur jeweiligen Problemlösung zu tun ist, sind dabei. Das ergibt den großen Mehrwert, der unsere Ressourcen intern schont. Wir nutzen das bereitgestellte Risk & Security Cockpit als zentrale Informations- und Kommunikationsplattform, rufen aber auch an, wenn es notwendig ist. Wir kommunizieren teilweise täglich mit den Analysten in Wien. Das Analysten-Team von RadarServices kommt zudem monatlich zu uns ins Haus. An diesen Terminen nehmen nicht nur wir aus dem IT-Sicherheitsbereich teil, sondern auch die Kollegen aus unseren operativen IT-Teams. Wir besprechen den Status der Datensammlung für das Monitoring, etwaige Veränderungen in der IT-Landschaft, Muster und Trends. Neben diesem engen Austausch mit den Analysten nehmen wir halbjährliche Meetings mit den Service Managern von RadarServices wahr. Das ist das Forum, in dem wir Strategisches und Verbesserungspotentiale besprechen.

Was sprach für einen Managed Service statt dem Aufbau eines hausinternen SOCs bei Red Bull?

Ein eigenes SOC bedeutet, dass wir mehrere hochspezialisierte Mitarbeiter für das Handling von Technologien, Prozessen und die Erkennung selbst an unserem Standort finden, langfristig halten und ihnen auch ständig die notwendigen fachlichen Herausforderungen bieten müssen. Das ist aus meiner Sicht für ein Unternehmen unserer Größe und mit einer ganz anderen Kernkompetenz als der IT-Sicherheit dauerhaft nicht machbar und sinnvoll. Daher war es keine Frage, dass wir mit externen Spezialisten arbeiten wollen. Und es ist bis heute die richtige Entscheidung.

As regards day-to-day IT security monitoring, you have relied on managed services provided by RadarServices for many years. This means your internal IT security team works together with security analysts from Europe's largest Security Operations Centre in Vienna every day. Exactly what form does this collaboration take?

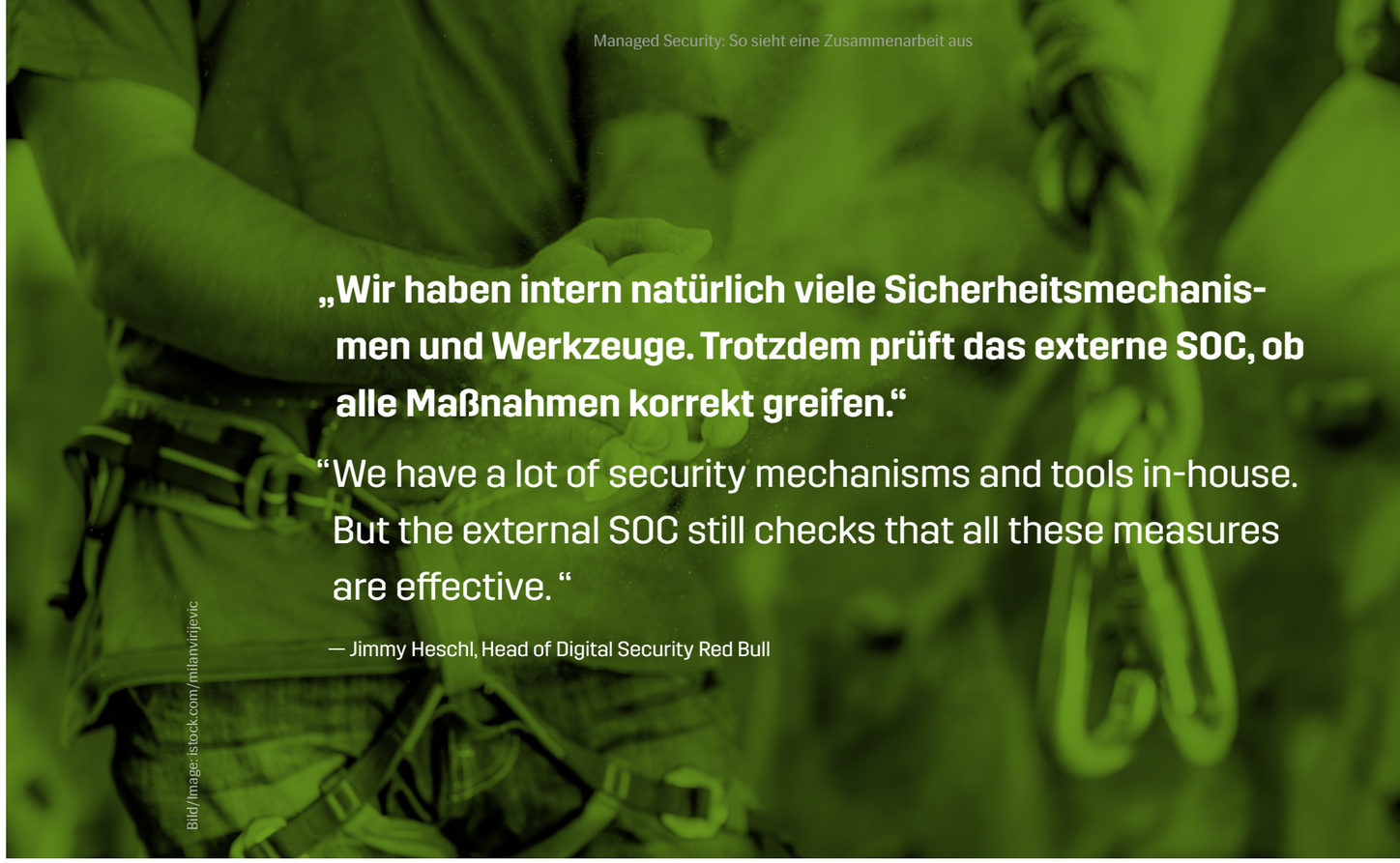
We communicate with the analysts in Vienna virtually every day. They pass on all the problems relevant to security that they have detected and prioritise and assess them for us. They also provide instructions to help us solve each individual problem. A major benefit of this is that it saves our in-house resources. They provide a risk & security cockpit which we use as a central information and communication platform, but we can also call them if we need to. We also get a monthly visit from the RadarServices' team of analysts. These IT security jour fixes are not only attended by us, but our colleagues from the operational IT team are also involved. We review the status of data collection for monitoring, changes to the IT landscape, patterns and trends. Beside these first-hand exchanges of information with the analysts, we also hold six-monthly meetings with the service managers of RadarServices. This provides a forum in which to discuss potential strategies and improvements.

What was the decisive factor for having a managed service, rather than setting up your own in-house SOC at Red Bull?

Having our own SOC would mean that we would have to find many highly-specialised security analysts to handle the technologies, the processes and the detection itself at our location, employ them long-term and also provide them with the professional challenges they need on an ongoing basis. I think that for a company of our size with key expertise that has nothing to do with IT security, this is neither feasible nor logical over the long term. So working with external specialists was never in doubt. And it remains the right decision to this day.

What considerations were crucial for the choice of your managed security services provider?

We see the ongoing collaboration with our external partner as one part of our security architecture. We



Was waren für Sie die entscheidenden Überlegungen bei der Auswahl Ihres Managed Security Services Providers?

Wir verstehen die kontinuierliche Zusammenarbeit mit unserem externen Partner als Teil unserer Sicherheitsarchitektur. Wir haben intern natürlich viele Sicherheitsmechanismen und Werkzeuge, die wir ständig verbessern. Trotzdem prüft das externe SOC, ob alle Maßnahmen korrekt greifen. Ist das nicht der Fall, werden wir informiert und falls notwendig alarmiert. Für uns sind die SOC-Leistungen also ein „zweites Sicherheitsnetz" aus einer unabhängigen Quelle.

Bei der Auswahl des konkreten SOC-Providers haben wir sehr genau abgewogen, wo wir lediglich Leistungen „von der Stange" kaufen würden und wo wir hingegen maßgeschneiderte Services und genügend Aufmerksamkeit bekommen. Die IT-Sicherheitslage jedes Unternehmens ist individuell und muss beim täglichen Balanceakt IT-Sicherheit auch von einem externen Serviceprovider in der Praxis so verstanden und gelebt werden. So sind wir zu RadarServices gekommen.

have a lot of security mechanisms and tools in-house, of course, and we are constantly adjusting and improving. But the external SOC still checks that all these measures are effective. They tell us if this is not the case, as well as alerting us, if necessary. Hence, we regard the SOC services as a "second line of defense" from an independent source.

We weighed things up meticulously when choosing an actual SOC provider – where would we merely be buying "off the peg" services, and where, on the other hand, would we get customised services and sufficient attention. The IT security situation at every company is different, and an external provider in the daily "IT security balancing act" also has to understand and live with this in practice. This is how we came to RadarServices.