Harald Reisinger, RadarServices

Simon Brickett, Computacenter

Photos: Computacenter, Claudia Panozzo

Worauf kommt's heute an?

Zwei Cyber Defence Strategen im gemeinsamen Interview

What is important today? – An interview with two cyber defence strategists

Simon Brickett leitet das Cyber Defence Centre in der Zentrale von Computacenter in London. Das Unternehmen ist einer der größten herstellerübergreifenden Dienstleister für alles rund um die IT von großen und mittelständischen, privaten und öffentlichen Organisationen in Europa. Harald Reisinger leitet die Cyber Defence Centres von RadarServices in Wien und – neu – in Vaduz (Liechtenstein). Der Geschäftsführer des am schnellsten wachsenden IT-Security Unternehmens in Europa arbeitet seit kurzem eng mit Simon Brickett und seinem Team zusammen. Im gemeinsamen Gespräch geben sie einen Einblick in das was ihre Kunden derzeit beschäftigt.

Herr Brickett, Computacenter ist der IT-Dienstleister für viele große Unternehmen in Europa und beliefert Kunden mit fast allem, was mit Hard- und Software zu tun hat. Was sind die wichtigsten Trends auf dem Security-Markt?

Simon Brickett: Es gibt viele Trends, die mit dem Tempo der Digitalisierung, des Technologiewandels und der sich weiterentwickelnden Bedrohungslandschaft zusammenhängen. Unsere Kunden sind auf der Suche nach umfassenderen, fortschrittlicheren und integrierten Plattform-Sicherheitslösungen. Um den ROI bestehender Sicherheitsinvestitionen zu erhöhen, ziehen sie dabei die „am besten integrierten" Detektions- und Reaktionsfähigkeiten in der Regel den „bestmöglichen" vor. Aufgrund der veränderten Compliance- und Datenschutzbestimmungen und des anhaltenden Fachkräftemangels erleben wir außerdem eine zunehmende Tendenz zum Outsourcing.

Sie entwickeln solche Plattform-Lösungen in Wien, Herr Reisinger, und sind mit dieser eigenen Technologie zum europäischen Marktführer geworden. Worauf kommt es Ihren Kunden an?

Harald Reisinger: Da gibt es vor allem drei ganz grundsätzliche Punkte: In erster Linie müssen Lösungen ganz klar Cutting-Edge sein. Deshalb haben wir von Anfang an eine hauseigene Researchabteilung aufgebaut. Sie beschäftigt sich mit Machine Learning und anderen Trends in der IT-Risikoerkennung. Durch sie werden die Erkenntnisse aus der weltweiten Forschung direkt in die Praxis umgesetzt. Ein zweiter wichtiger Punkt: Es geht um Vertrauen. Wenn man IT-Risikoerkennungstechnologie einkauft, will man in erster Linie Sicherheit und kein neues Risiko. Durch unsere interne Entwicklung bieten wir jedem Kunden die Möglichkeit, jede Codezeile in unserer Software genau nachvoll-

Simon Brickett heads the Cyber Defence Centre at the Computacenter headquarters in London. The company is one of the largest cross-manufacturer service providers for everything to do with IT for large and medium-sized, private and public organisations in Europe. Harald Reisinger is in charge of the Cyber Defence Centres of RadarServices in Vienna and – now – in Vaduz (Liechtenstein). The Managing Director of Europe's fastest growing IT security company has recently started working closely with Simon Brickett and his team. In an interview together, they give an insight into the issues their customers are currently dealing with.

Mr. Brickett, Computacenter is the IT service provider for many large companies in Europe supplying customers with almost everything to do with hardware and software. What are the major trends they see in the security market?

Simon Brickett: There are many trends linked to the pace of digitalization and technology change and the evolving threat landscape. Our customers are looking for deeper, more advanced and integrated platform security solutions. They also want "best integrated" detection and reaction capabilities rather than "best of breed" to help with ROI from existing security investments. We are also seeing an increasing tendency to outsource because of the changes in compliance and data privacy regulation and the ongoing skills shortage.

Mr Reisinger, you develop such platform solutions in Vienna and have become Europe's market leader with the in-house developed technology. What is important to your customers?

Harald Reisinger: There are particularly three factors in focus: First and foremost, technology needs to be cutting-edge at any point of time. This is why we have built up an in-house research department right from the start of our company. The department is involved in machine learning and other trends concerning IT risk detection technology. Latest advances from global research are immediately put into practice. Second, it's a matter of trust. When you purchase IT risk detection technology, you primarily want security and no new risk. We have our software development team in-house. Each of our customers may review every line of software code in detail. No US provider offers such in-depth insights. However such transparency is very important to be sure that there are no backdoors in the software. The third point concerns the "big picture" of IT security in an organization:

ziehen zu können. Das bietet kein amerikanischer Anbieter, ist aber immens wichtig, um sicher sein zu können, dass es keine Hintertürchen in der Software gibt. Der dritte Punkt betrifft das „Big Picture" der IT-Sicherheit in einer Organisation: Unsere Technologie bringt alle sicherheitsrelevanten Informationen – sowohl aus bestehenden Lösungen als auch neuen Werkzeugen – zusammen in ein zentrales Cockpit. Es gibt keine Datensilos und keine blinden Flecken mehr.

Herr Brickett, die Nutzung der Cloud ist für die Kunden von Computacenter ein großes Thema. Was sind die sicherheitsrelevanten Themen rund um die Cloud, die Ihre Kunden betreffen?

Simon Brickett: Unsere Kunden, die bereits viele Cloud-Lösungen im Einsatz haben, sind auf der Suche nach einer größeren Skalierbarkeit und besser abgestimmten Geschäftsmodellen, um ihre Investitionen zu optimieren. Da IT-Sicherheit ein komplexes Unterfangen ist und von Anfang an mitgedacht werden muss, bitten uns Unternehmen häufig, sie bei der Auswahl der richtigen strategischen Sicherheitslösungen zu unterstützen. Andere Kunden, die bei der Implementierung von Cloud-Lösungen noch am Anfang stehen, sind noch dabei, traditionelle Sicherheitsmodelle an die neuen Arbeitsweisen anzupassen und die Auswirkungen auf den Datenschutz, die Prozesssicherheit bei maximaler Auslastung der Cloud-Lösungen und neue Bedrohungsvektoren zu verstehen.

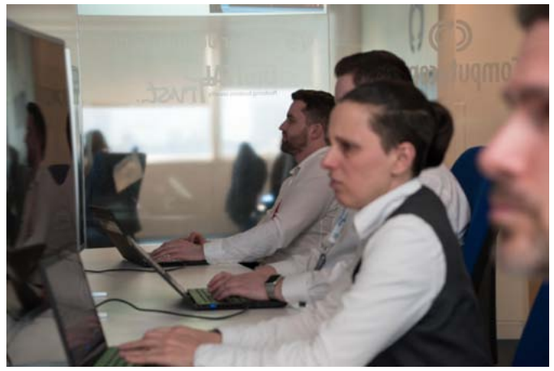
we gather all security-related information – both from existing solutions and new tools – in one central cockpit. Data silos and blind spots are things of the past.

Cloud use is also a big issue for your customers. What are the security-related issues around the cloud that concern your customers?

Simon Brickett: Our mature cloud adopter customers are looking for more scale and better commercial models to optimise their investments. Here, as security is often wrongly considered a limiting factor, we are asked to help companies identify the right strategic security solutions to enable their business. Other less mature customers are still adapting traditional security models to new ways of working and are trying to understand the impact on data privacy, securing workloads and new threat vectors.

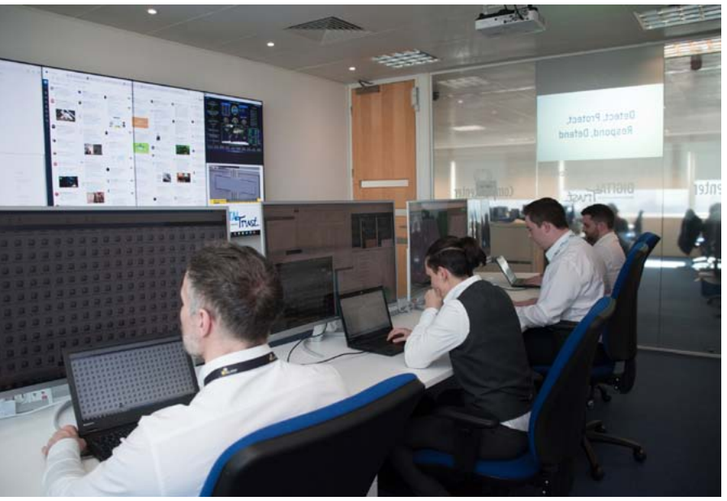
You work with many manufacturers worldwide. How far has "Security by Design" progressed in practice?

Simon Brickett: We work with most major vendors and we resell their products, design, build and implement solutions with their software, and manage services built on their technology. At every stage of these engagements we see vendors embed-



Volle Konzentration im Computacenter Cyber Defence Centre
Highly concentrated analysts in the Computacentrer Cyber Defence Centre

Photos: Computacenter



Sie arbeiten mit vielen Herstellern weltweit zusammen. Wie weit ist „Security by Design" in der Praxis fortgeschritten?

Simon Brickett: Wir arbeiten mit den meisten großen Herstellern zusammen – vertreiben ihre Produkte, konzipieren, entwickeln und implementieren Lösungen mit ihrer Software und verwalten Services, die auf ihrer Technologie basieren. In jedem dieser Bereiche gibt es Anbieter, die Sicherheit von Anfang an in ihre Produkte integrieren. Ein gutes Beispiel sind Windows 10 und O365, die mit wirklich eindrucksvollen Sicherheitsfunktionen ausgestattet sind. Es gibt aber noch viel zu tun, da jeder Kunde andere Sicherheitsanforderungen hat und wir immer noch Lücken entdecken, die wir schließen können. Bei anderen Herstellern geht es bei „Security by Design" mehr darum, SecDevOps zu ermöglichen und sicherzustellen, dass die Implementierung und der Betrieb von Sicherheit ein agiler Prozess ist.

„Security by Design" ist auch bei IIoT – Industrial Internet of Things – ein immer wichtigeres Thema. Maschinen haben komplexe Steuerungssysteme und sind in puncto Sicherheit für Kunden schwer durchschaubar. Wie kann man sie vor Angriffen schützen?

Harald Reisinger: Produktionsunternehmen sind hochgradig digitalisiert und damit von einer ständig funktionierenden Operational Technology abhängig. Wie viel Sicherheit jede einzelne Maschine herstellerseitig mit sich bringt, ist jedoch für die Zuständigen in der Produktion oft nicht nachvollziehbar. Daher ist es wichtig, dass sicherheitsrelevante Ereignisse und Netzwerkverkehr – ähnlich wie bei der IT – kontinuierlich überwacht werden. Auffälligkeiten können nur so festgestellt, frühzeitig nach Lösungsmöglichkeiten gesucht und Schäden oder Stillstand verhindert werden.

Herr Brickett, was sagen Sie: Leben wir in goldenen Zeiten für Hacker?

Simon Brickett: Die These ist sicher nicht ganz falsch, denn es gibt deutlich mehr Möglichkeiten für Hacker: neue Bedrohungsvektoren, Advanced Persistent Threats und eine stetig zunehmende Zahl potenzieller Einfallspunkte durch das Internet of Everything. Aber die gute Nachricht ist, dass die „gute Seite" auch immer besser wird, nicht nur aus technologischer Sicht, sondern auch in Bezug auf Wissen und Fähigkeiten. Was uns die aktuellen Trends meiner Meinung nach zeigen, ist, wie zentral für Unternehmen die Herausforderung ist, die richtigen und ausreichend hoch qualifizierten Mitarbeiter zu gewinnen. Wenn der Fachkräftemangel dies nicht zulässt, sollten Unternehmen über alternative Sourcing-Modelle, wie zum Beispiel Managed Security Services, nachdenken.

ding security into their products. A good example is Windows 10 and O365 which comes with really exciting security features. There is still work to do, as all customers have different levels of security requirements, and we still see gaps we can help to close. For other vendors, security by design is more about enabling SecDevOps and working to ensure that implementing and operating security is an agile process.

"Security by Design" has become an increasingly important topic for IIoT – the Industrial Internet of Things. Machines have complex control systems and security sometimes rather a "black box". How can you protect them from attacks?

Harald Reisinger: The manufacturing sector is highly digitalized and therefore depends on a constantly functioning Operational Technology. How secure each machine is, however, is often incomprehensible for the responsibles in a plant. It is important that security-related events and network traffic are continuously monitored – similar to the monitoring of an IT infrastructure. This is how anomalies can be detected early on and damages or a standstill are prevented.

Mr. Brickett, what do you think: Do we live in golden times for hackers?

Simon Brickett: I think that's probably a fair assessment, with new threat vectors, Advanced Persistent Threats and the increasing numbers of potential entry points courtesy of the Internet of Everything, there is a lot more opportunity for hackers. But the good news is the good guys are getting better as well, not only from the technology point of view, but we are also seeing improving skills sets as well. But what I think the current trends do show us is that it is paramount for organizations to hire the right, highly skilled people. If they lack them, it's better to think about sourcing alternatives such as Managed Security Services.