Bildnachweis: © Lukas Dostal

Christian Polster, Chefstratege bei RadarServices über den Schutz von Unternehmensdiamanten

„Viele Organisationen sind sich ihrer Diamanten-schätze nicht bewusst – und schützen sie dement-sprechend schlecht!“

IT-Landschaften von Unternehmen und Behörden sind groß, sehr groß. Alle Systeme und Daten gleichermaßen auf höchstem Niveau zu schützen, ist ein Ziel, welches kaum eine Organisation in der Praxis nachhaltig erreicht. Die Frage ist, ob dieser Ansatz überhaupt der Richtige ist. Christian Polster, Chefstratege und verantwortlich für die Technologieentwicklung beim IT Security Spezialisten RadarServices spricht über das Bewusstsein und das Schutzniveau von Unternehmensdiamanten in der europäischen Wirtschaft und seinen Grundgedanken für den Schutz der besonders kritischen „Assets“ einer Organisation.

Christian Polster, chief strategist at RadarServices on the protection of corporate diamonds: “Many organisations are unaware of their diamond treasures – and protect them correspondingly poor!” – The IT landscapes of companies and authorities are big, very big. Ensuring that all systems and data are fully protected to the highest standards at all times is a goal that virtually no company is able to achieve on a sustainable basis. The question is whether such an approach is indeed even the right one. Christian Polster, chief strategist and responsible for technology development at IT Security specialist RadarServices, speaks about the level of awareness and protection of corporate diamonds in the European economy and his basic idea for protecting the most critical “assets” of an organisation.

Herr Polster, um die Entwicklung Ihrer IT-Risikoerkennungstechnologie an den Bedürfnissen Ihrer Kunden auszurichten, stehen Sie im ständigen Austausch mit IT-Sicherheitsverantwortlichen in Unternehmen aus vielen verschiedenen Branchen und dem öffentlichen Sektor. Wie fassen Sie das aktuelle Schutzniveau in der europäischen Wirtschaft generell zusammen?

Cybersecurity ist in vielen Organisationen weit oben auf der Agenda. Es wird viel investiert und getan. Industrieunternehmen sind Vorreiter. Banken und Versicherungen sind aufgrund der umfassenden Compliancevorschriften seit Jahren aktiv. Trotzdem ist das Schutzniveau von Unternehmen zu Unternehmen sehr unterschiedlich. „Es wird uns schon nicht erwischen“, höre ich immer noch des Öfteren, wenn ich Unternehmen zum ersten Mal besuche und unsere Leistungen vorstelle. „IT-Sicherheit ist wichtig, aber es darf nur sehr wenig kosten“, auch von Zeit zu Zeit. Deshalb kann ich kein durchgehend positives Bild einer sicheren europäischen Wirtschaft zeichnen. Es gibt leider viel Angriffsfläche und sie wird auch im Rahmen von immer zahlreicher und komplexer werdenden Attacken ausgenutzt.

Worauf sollten sich Unternehmen in punkto IT-Sicherheit konzentrieren?

Jedes Unternehmen hat seine “Diamanten”, also die besonders kritischen Daten, Systeme, Geschäftsgeheimnisse oder Prozesse – kurz „Assets“. Konstruktionspläne, Patente, Kundendaten, Patientendaten, Baupläne oder Finanzdaten gehören zum Beispiel dazu. Diese Assets gilt es auch IT-seitig ganz besonders abzusichern. Je weiter sich die Digitalisierung fortsetzt, desto mehr müssen IT-Sicherheitsverantwortliche selektieren, welche Systeme, Daten und Applikationen welchem Sicherheitsniveau unterliegen müssen. Es wird nicht mehr möglich sein, alles gleichermaßen abzusichern. Gleichzeitig müssen die kritischen Assets hervorragend gesichert sein.

Hier beginnt das Problem: Organisationen wissen heute meist nicht, was genau zu ihren „Diamanten“ gehört und welche Systeme, Daten oder Applikationen besonders gut gesichert sein müssen, damit potentiell existenzgefährdende Risiken wie der Verlust von Kundenvertrauen in eine Marke oder ein Produkt vermieden werden. IT-Sicherheit wird heute als technisches Problem mit einer technischen Lösung gesehen. Der Zusammenhang der IT mit den eigentlichen Geschäftsabläufen in einer Organisation und den Unternehmenswerten fehlt sehr oft. Diese Lücke muss aber geschlossen werden, um sicherheitsseitig für die weitere Digitalisierung gerüstet zu sein. Nur so schafft man es, die kritischen Assets adäquat zu schützen.

Bei den Investitionen, die Organisationen im Bereich Cybersecurity eingehen, ist also weniger manchmal mehr?

So ist es! Unternehmenslenkern wird mehr und mehr bewusst, wie vielfältig Angriffsarten und Einfallstore und wie herausfordernd die Zukunft der Digitalisierung – Stichwort IoT oder künstliche Intelligenz – ist. Sie investieren daher auch stetig mehr in IT-Sicherheit. Dadurch werden ihre kritischen Assets aber nicht zwingend besser geschützt. Auch Investitionsentscheidungen sollten nicht nur aus der „technologischen Brille“ gesehen werden, sondern immer auch vor dem Hintergrund ihres Nutzens für den Schutz der eigenen Unternehmensdiamanten.

Wie trifft man vor diesem Hintergrund die richtigen Entscheidungen?

Es bedarf einiger Vorarbeit, um die kritischen Assets in einer Organisation zu identifizieren. Sie werden von den Geschäftsprozessen und Unternehmenswerten hergeleitet, die ihrerseits oftmals vielschichtig sind und verschiedene Unternehmenseinheiten, Personen und Länder involvieren oder unterschiedliche Rahmenbedingungen haben. Assets sind also je nach Branche und je nach Organisation unterschiedlich. Die in der Realität existierende Komplexität sollte auch nicht reduziert werden, da dadurch wichtige Faktoren für die IT-Sicherheit der kritischen Assets beeinträchtigt werden könnten. Für diese Vorarbeit ist eine Involvierung verschiedener interner Stakeholder und externer Fachexperten empfehlenswert.

Die selektierten Assets sollten dann einem umfassenden Risikocheck unterzogen werden: Welchem Risiko sind sie ausgesetzt, welche Angreifer könnten ein Interesse verfolgen, die Assets zu attackieren und wie gut geschützt sind die Assets durch die aktuellen Sicherheitsmaßnahmen? So kommt man sukzessive zu einer klaren Roadmap, wo gänzlich „blinde Flecken“ bei den aktuellen Sicherheitsmaßnahmen sind, wonach zu justieren ist oder wo gegebenenfalls auch Potential zur Reduktion von Security-Investitionen ist ohne dass das Schutzniveau für kritische Assets bedenklich sinkt.

Wesentlich für diesen Ansatz der IT-Risikoevaluation ist also die Herangehensweise ausgehend von der Bestimmung der „Unternehmensdiamanten“ statt der Technologie. Im nächsten Schritt betrachtet man die Diamanten aus verschiedenen Perspektiven: Der Wichtigkeit für interne und externe Stakeholder und auch der Attraktivität für Angreifer. Und schlussendlich entsteht eine Prioritätenliste an Aufgaben, benötigten Technologien und auch eine Feedbackschleife zu den aktuell vorhandenen IT-Sicherheitsmaßnahmen.

Mr Polster, in order to align the development of your IT risk detection technology with the needs of your customers, you are in constant contact with IT security officers in companies from many different industries and the public sector. How would you summarise the current level of protection in the European economy in general?

Cyber security is high on the agenda in many organisations. There is a lot of investment and action here. Industrial companies are pioneers. Banks and insurance companies have been active here for years due to extensive compliance regulations. Nevertheless, the level of protection varies greatly from company to company. “It won’t affect us,” is something I still often hear when I visit companies for the first time and introduce our services. “IT security is important, but it mustn’t cost very much,” I am also told from time to time. That is why I cannot draw a consistently positive picture of a secure European economy. Unfortunately, there is a large attack surface and it is also being exploited through increasingly numerous and complex attacks.

What should companies focus on in terms of IT security?

Every company has its “diamonds”, i.e. highly critical data, systems, business secrets or processes – in short “assets”. It must be a special focus of IT to protect these in particular. The further digitisation progresses, the more IT security officers have to decide which systems, data and applications must be subject to which security level. It will no longer be possible to secure everything to the same extent. At the same time, critical assets must be extremely well secured.

This is where the problem begins. Mostly, organisations today are not aware of what exactly their “diamonds” are or which systems, data or applications must be particularly well secured to avoid risks that may endanger the continued existence of the company, such as the loss of customer confidence in a brand or product. IT security is today seen as a technical problem with a technical solution. The relationship between IT and the actual business processes in an organisation and company values is very often missing. This gap must be closed, however, in order to be prepared for further security-related digitisation. This is the only way to appropriately protect the critical assets.

So, in terms of the investments that organisations make in cyber security, less is sometimes more?

That is correct. Business leaders are becoming increasingly aware of the variety of types of attacks and points of entry, and how challenging the future of digitisation is – think IoT or artificial intelligence. As a result, they are investing more and more in IT security, yet this does not necessarily protect their critical assets better. Investment decisions should not only be seen through “technological glasses”, but always in terms of the benefits they convey for the protection of their own company diamonds.

With this in mind, how do you make the right decisions?

Some preliminary work is needed to identify the critical assets in an organisation. They are derived from business processes and corporate values, which are often complex and involve different business units, people and countries, or have different framework conditions. Assets therefore vary by industry and organisation. Nor should the complexity that exists in reality be reduced, as it could negatively affect critical IT asset security factors. The involvement of various internal stakeholders and external experts is recommended when carrying out this preliminary work.

The selected assets should then be subjected to a comprehensive risk check: what risks are they exposed to, which attackers could have an interest in attacking the assets and how well protected are the assets by the current security measures? This process leads to the gradual creation of a clear roadmap of where there are currently complete “blind spots” in the current security measures, where adjustments need to be made or, where appropriate, there is also potential to reduce security investments without the level of protection for critical assets sinking drastically.

The approach based on the determination of “corporate diamonds” rather than technology is therefore essential to this approach of IT risk evaluation. In the next step, the diamonds are considered from different perspectives: the importance for internal and external stakeholders and attractiveness for attackers. Finally, a priority list of tasks, required technologies and a feedback loop on the current IT security measures is created.