Bild/Image: RR Power Systems AG

„Disruptive technologies und IT-Sicherheit: Wie kann man Unternehmensdaten schützen, wenn man nicht sicher weiß, wo sie liegen?"

Lothar Hänsler, IT Security Officer bei Rolls-Royce Power Systems AG, zu den Zukunftstrends im Interview

"Disruptive technologies and IT security: How can you protect company data if you don't know for sure where they are?" An interview about future trends with Lothar Hänsler, IT Security Officer at Rolls-Royce Power Systems AG

Die großen, strategischen Zusammenhänge mit den kleinen, tieftechnischen Details zusammenzubringen, das ist die Spezialität von Lothar Hänsler – diesen Eindruck vermittelt er, wenn man ihn zum Thema IT-Sicherheitstrends anspricht. Ein Vordenker mit Experten-Know-how und damit ein hochinteressanter Gesprächspartner, um der Antwort auf die Frage nach den goldenen Zeiten näher zu kommen.

Lothar Hänsler ist IT Security Officer bei Rolls-Royce Power Systems AG, dem Spezialisten für Großmotoren, Antriebssysteme und dezentrale Energieanlagen. Das Unternehmen mit Hauptsitz in Friedrichshafen beschäftigt über 10.000 Mitarbeiter weltweit und ist ein Geschäftsbereich von Rolls-Royce plc.

Herr Hänsler, welche Rolle spielt die IT heute im Motorenbau?

Bei Rolls Royce Power Systems/MTU ist der Grad der IT-Durchdringung sehr hoch und deckt alle Bereiche des Unternehmens ab. Integrierte ERP-Lösungen tangieren Einkauf, Produktion, Vertrieb, Rechnungswesen bis hin zu HR, Legal und Compliance. Ich kann nicht für die gesamte Branche sprechen, aber ich nehme an, dass es bei anderen Unternehmen ähnlich ist.

Im Zuge der Digitalisierung nimmt die Durchdringung mit IT-Lösungen noch einmal deutlich zu: Industrie 4.0, IoT, Cloud Computing, Mobility, Analytics, AI usw. Die Schlagworte geistern durch die Medien und sind bekannt.

Was sind die großen Themen in punkto IT-Sicherheit, die Sie besonders beschäftigen?

Die „Disruptive Technologies" beschäftigen mich sehr. Mobile Computing, Cloud Computing, IoT, IIoT (Industrial Internet of Things) und Industrie 4.0 gehören dazu. Warum? Weil in diesen Bereichen Komponenten ins Spiel kommen, die per se nicht auf „Security by Design" aufbauen, aber an vorderster Front eingesetzt werden. Man spricht ja auch vom „Fluid Perimeter". Das heißt, dass die Grenze eines Unternehmensnetzes nicht mehr so einfach feststellbar ist. Mit dem Einsatz von IoT-Geräten, Cloud-Lösungen usw. wächst also die Herausforderung, den Gesamtüberblick zu behalten und die Daten eines vernetzten Unternehmens weiterhin angemessen zu schützen.

Die Technologien, die in Produktionsunternehmen heute im Einsatz sind, kommen von verschiedenen Herstellern, deren IT-Sicherheit wir als Kunden einschätzen müssen. Das ist keine leichte Aufgabe. Einerseits weil es so komplexe und unterschiedliche Lösungen sind. Andererseits weil der Fachkräftemangel im Bereich IT-Sicherheit noch spürbarer wird, wenn es um Know-how für neue Technologien geht.

Bringing together the broad, strategic thinking with the small, technical details: this is the speciality of Lothar Hänsler. An impression he conveys when you talk with him about IT security trends. A leading thinker with expert know-how and thus a highly interesting discussion partner to consider the answer to the issue of golden eras.

Lothar Hänsler is the IT Security Officer at Rolls-Royce Power Systems AG, the specialist for large engines, propulsion systems and decentralised energy systems. Based in Friedrichshafen, Germany, the company employs over 10,000 people worldwide and is a division of Rolls-Royce plc.

Mr Hänsler, what role does IT play today in engine construction?

At Rolls Royce Power Systems/MTU, the level of IT penetration is very high, covering all areas of the business. Integrated ERP solutions cut through Purchasing, Production, Sales and Accounting all the way to HR, Legal and Compliance. I can't speak for the industry as a whole, but I assume it is a similar situation for other companies.

IT solutions are reaching an even higher degree of penetration in the course of digitalisation: Industry 4.0, IoT, Cloud Computing, Mobility, Analytics, AI etc. Keywords that echo throughout the media and are well-known.

What are the major issues relating to IT security that you focus on particularly?

I focus particularly on what are known as disruptive technologies. These include Mobile Computing, Cloud Computing, IoT, IIoT (Industrial Internet of Things) and Industry 4.0. Why? Because components are used in these areas that are not based on "security by design" per se, but are used on the front line. People also speak of a fluid perimeter here. This means that it is no longer easy to see where the boundaries of a company's network are any more. Using IoT devices, cloud solutions, etc. also means that there is a greater challenge to keep sight of the overall picture and to continue protecting the data of a networked company to an appropriate extent.

Technologies that are used in production companies today come from different manufacturers with a level of IT security that we as customers must assess. This is no easy task. On the one hand, this is because they are complex and varied solutions. On the other, it is because the lack of experts in the field of IT security becomes even more tangible when it comes to know-how regarding new technologies.

For example: Introducing agile methods can pose particular

Photo: RR Power Systems AG

Dezentral Energieanlage von Rolls-Royce Power Systems AG, hier: Vor-Ort-Strom-Datenzentrum Amsterdam
Rolls-Royce Power Systems AG decentralised energy system, here: onsite energy data centre Amsterdam

Ein Beispiel: Die Einführung agiler Methoden kann besondere Herausforderungen an die IT-Sicherheit darstellen. Hoher Termindruck und flexible Vorgehensmodelle führen zum Risiko, dass bei einem Hersteller in der Eile nicht immer sorgfältig genug vorgegangen werden kann. In Kombination mit den disruptiven Technologien kann daraus schnell eine gefährliche Kombination entstehen.

Ein weiteres Stichwort: Cloud-Dienste. Hier sind die Veränderungszyklen auf der Herstellerseite derart rasant, dass eine systematische und fundierte Prüfung von Sicherheitsmechanismen kaum mehr möglich ist. Das deutsche Bundesamt für Sicherheit in der Informationstechnik – kurz BSI – hat in diesem Bereich das Konzept des C5-Attestats eingeführt. Ich halte das für einen guten Schritt. Cloud-nutzenden Unternehmen wird dadurch ein Status der IT-Sicherheit beim Cloud-Provider vermittelt. Dennoch reduziert es die IT-Sicherheit auf eine „Prüfung der Papierform".

Im Bereich der mobilen Anwendungen ist ein Trend erkennbar, dass diese Softwaresysteme zu „Apps" verniedlicht werden. Es wird suggeriert, dass die Entwicklung solcher Anwendungen einfach sei und sich das quasi jeder aneignen kann. Best Practices wie ein sicherer Softwareentwicklungsprozess, Security by Design, Privacy by Design fallen so aber eventuell unter den Tisch.

Diesen und ähnlichen Herausforderungen stellen wir uns, um unsere IT-Sicherheitsstandards hoch zu halten.

Welche weiteren strategischen Herausforderungen sehen Sie auf Unternehmen Ihrer Branche in Sachen IT-Sicherheit zukünftig zukommen?

Da gibt es viele Schlagworte aus ganz verschiedenen Bereichen. Hier einige Wichtige davon:

Die wachsenden Standardisierungsbemühungen auf globaler Ebene führen im IT-Sicherheitsbereich nicht nur zu Vereinfachungen. Öffentliche Auftraggeber publizieren zunehmend eigene Standards und verlangen von ihren Lieferanten deren Einhaltung. Das stellt international agierende Unternehmen vor besondere Herausforderungen. Die Einhaltung eines Standards ist dann nicht ausreichend, um unterschiedliche Auftraggeber zufriedenzustellen. Es wäre einfacher, wenn diese an sich notwendigen Standards zu einem „überschaubaren" Katalog an Anforderungen geführt würden.

Hinzu kommen internationale, sich ständig ändernde Regularien zu IT-sicherheitsrelevanten Themen, so zum Beispiel zu Verschlüsselung oder Aus- und Einfuhrbeschränkungen für Hardware und Software.

Andererseits gibt es eine starke Abhängigkeit von der Supply Chain, also der Versorgung des Unternehmens mit Lieferantenleistungen. Die Supply Chain Security wird daher strategisch immer wichtiger. „Chain" steht für „Kette" und die Kette ist nur so stark wie das schwächste Glied. Unternehmen dürfen sich nicht mehr in Sicherheit wiegen, weil die eigene Sicherheitstechnologie „State of the Art" ist. Zu einer ganzheitlichen Betrachtung gehört auch die Bewertung der IT-Sicherheit von Dienstleistern, Fernwartungsunternehmen, Beratungshäusern, Anwaltskanzleien und vielen mehr.

In diesem Zusammenhang – aber auch ganz generell – bereiten die Entwicklungen hin zur Cloud doch vielen Sicherheitsverantwortlichen Kopfschmerzen. „Es prüfe, wer sich ewig bindet": Die Gefahr des Vendor-Lock-Ins, also der Unmöglichkeit den Cloudanbieter wechseln zu können, wenn man seine Daten einmal in der Cloud abgelegt hat, ist eines der großen Risiken.

Eine ganz andere Herausforderung ergibt sich aus den politischen Entwicklungen in der jüngeren Vergangenheit: Einfuhrzölle und Abschottungsmaßnahmen haben nicht nur weltwirtschaftliche Auswirkungen. Sie zwingen Unternehmen unter anderem

challenges to IT security. Pressure to meet deadlines and flexible approach models lead to the risk that, in its haste, a manufacturer may not be able to proceed with a sufficient degree of care. Combined with disruptive technologies, this can quickly result in a dangerous combination.

Another keyword here: cloud. Manufacturer change cycles are currently so fast that it is scarcely possible to conduct a systematic and in-depth inspection of security mechanisms. The German Federal Office for Information Security (BSI) has introduced the C5 certification concept in this area. This is definitely a step in the right direction. This gives cloud-using companies confirmation of the IT security status of a cloud provider. Nevertheless, this reduces IT security to an "audit on paper".
In the area of mobile applications, there is a trend towards these software systems being reduced to "apps". It is suggested that developing such applications is simple and can be acquired by virtually anyone. This means, however, that best practices such as a secure software development process, security by design, privacy by design might fall by the wayside.

We take these and other challenges to keep our own IT security standards at a high level.

What other strategic challenges do you see being faced by companies in your industry in terms of IT security in the future?

There are many keywords here from a whole host of different areas. Here are a few important ones:

Growing standardisation efforts at a global level do not only lead to simplifications in the area of IT security. Public-sector customers are increasingly publishing their own standards and requiring their suppliers to comply with them. This poses internationally active companies with particular challenges, as it is then not enough to comply with one standard to satisfy different customers. It would be simpler if these standards, which are basically required, are compiled in a "manageable" catalogue of requirements.

On top of this come international, ever-changing regulatory frameworks regarding topics concerning IT security, such as encryption or export and import restrictions for hardware and software.

On the other hand, there is a high degree of dependency on the supply chain, i.e. supplying the company with vendor services. This means that supply chain security is becoming increasingly important from a strategic standpoint. As we know, a chain is only as strong as its weakest link. It is not enough for companies to believe they are secure because their own technology is state-of-the-art. Taking a holistic view also means assessing the IT security of service providers, remote maintenance companies, consultancies, law firms, and many more.

With this in mind – but also generally speaking – the trend towards cloud computing is causing a headache for many security officers. "Commit in haste, repent at leisure": The risk of vendor lock-in, i.e. the inability to change cloud provider once you have stored your data in the cloud, is one of the greatest risks.

Political developments in recent times represent a very different kind of challenge: import duties and protectionist measures do not just affect the global economy. They also force companies to have to be flexible in the field of security and to get used to the idea that it may not be possible to obtain security technologies from known sources for an indefinite period of time. Changes in the political landscape may quickly result in individual countries being viewed as (potential) attackers.

Politically motivated cyber attacks are already commonplace today. They show what attackers are already capable of today

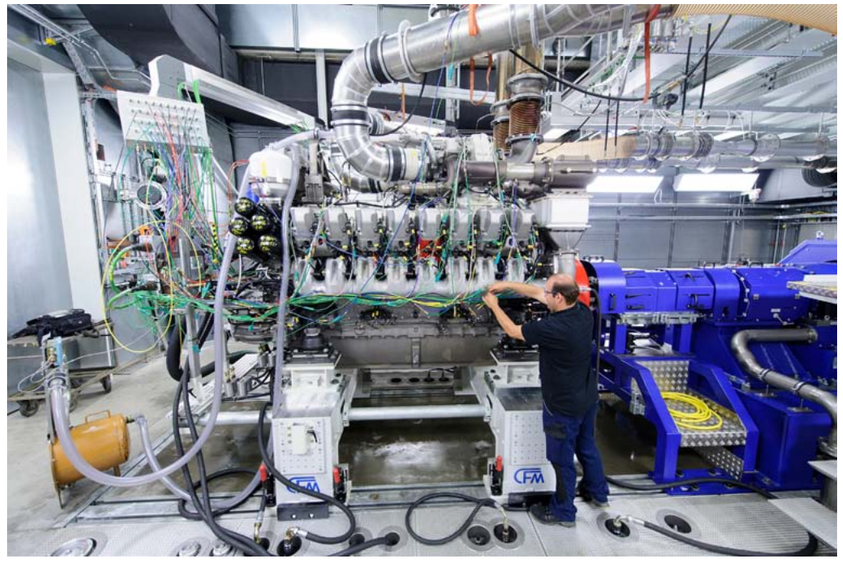

Photo: RR Power Systems AG

Rolls-Royce Power Systems AG, Großmotoren, hier: Auf dem Prüfstand
Rolls-Royce Power Systems AG large engine, here: on the testbench

auch dazu, im Sicherheitsbereich flexibel sein zu müssen und sich darauf einstellen zu müssen, dass Sicherheitstechnologien nicht zeitlich unbegrenzt aus bekannten Quellen bezogen werden können. Änderungen in der politischen Großwetterlage können schnell dazu führen, dass einzelne Länder als (potenzielle) Angreifer betrachtet werden müssen.

Politisch motivierte Cyberangriffe sind heute schon allgegenwärtig. Sie zeigen, welche Möglichkeiten Angreifer heute schon haben und worauf sich Unternehmen für die Zukunft einstellen müssen. Sicherheitsverantwortliche müssen in dieser Hinsicht weit über den Tellerrand hinausschauen und jenseits der internen Sicherheitstechnologien denken.

Durch den anfangs erwähnten, zunehmend poröser werdenden Perimeter aufgrund von IoT, Cloud usw. ist es wichtig, Transparenz zu haben, wo die Daten des Unternehmens abgelegt sind und wer darauf Zugriff hat. Im Zuge der Einführung der EU-DS-GVO wurde dies unter der Überschrift „Data Mapping“ adressiert. Die Wichtigkeit einer solchen Transparenz kann nicht überbetont werden: Wie kann man die Unternehmensdaten schützen, wenn man nicht sicher weiß, wo sie liegen?

Artificial Intelligence ist auch eines der Buzzwords, die derzeit durch die Presse gehen. In diesem Ansatz steckt auch ganz sicher ein großes Potenzial. Sicherheitsverantwortlichen legt er aber auch Sorgenfalten auf die Stirn: Wann werden wir die ersten Angriffe auf AI-Basis sehen, die alle bisher bekannten Verteidigungsmittel in den Schatten stellen, weil die Angriffswerkzeuge während des Angriffs lernen, wie sie die Verteidigungsmaßnahmen lahmlegen können?

Daneben deuten die Fortschritte im Bereich Quanten-Computing darauf hin, dass wir in absehbarer Zeit Alternativen zu den bisherigen Verschlüsselungstechnologien brauchen werden. Auch hier stellt sich die Frage, wer das Rennen in diesem Katz-und-Maus-Spiel zwischen Angreifer und Verteidiger gewinnen wird.

Herr Hänsler, leben wir derzeit in „goldenen Zeiten“ für Hacker?

Absolut. Die explosionsartige Verbreitung der Vernetzung von tendenziell unsicheren Komponenten im IoT-Umfeld, kombiniert mit immer schnelleren Entwicklungszyklen und extrem schnellen Veränderungen in der Cloud-Infrastruktur erhöht die Angriffsfläche. Die Entwicklung im AI-Bereich wird auch auf der Angreiferseite ausgenutzt. Bessere Angriffswerkzeuge treffen auf immer mehr angreifbare Plattformen, das alles in einem international vernetzten Raum, in dem die Strafverfolgung oft an Landesgrenzen scheitert. Wenn das nicht goldene Zeiten sind?

and what companies need to be prepared for in the future. In this regards, security officers need to think outside the box and look beyond internal security technologies.

As a result of increasingly porous perimeter caused by IoT, cloud systems, etc., mentioned at the beginning, it is important to have transparency regarding where the company's data are stored and who has access to them. This issue was addressed under the heading "data mapping" in the course of introducing the EU GDPR. The importance of such transparency cannot be stressed enough: How can you protect company data if you don't know for sure where they are?"

Artificial intelligence is also a buzzword that we are currently seeing a lot of in the media. There is definitely a lot of potential hidden in this approach. However, security officers are deeply concerned here: When we will see the first attacks using AI that completely eclipse all known defence mechanisms because the attacking software is able to learn, during the attack, how to paralyse these defences?

In addition, progress in the area of quantum computing suggests that, in the foreseeable future, we will need alternatives to the encryption technologies currently available. This also begs the question of who will win this game of cat-and-mouse: the attackers or the defenders?

Mr Hänsler, are we currently in a “golden age” for hackers?

Absolutely. The explosive growth of the interconnectedness of rather insecure components in the IoT environment combined with increasingly rapid development cycles and extremely fast changes of cloud infrastructure present an ever-growing target. The developments in the area of A.I. will be exploited by cyber-attackers as well. Sophisticated attacking tools encounter more and more vulnerable platforms, this happens in an internationally networked space where criminal prosecution fails due to national borders. If these are not golden times?

Rolls-Royce Power Systems AG Energieanlage, Hier: Kraftwerk, Bangladesh, Chittagong
Rolls-Royce Power Systems AG energy system, Here: power plant, Bangladesh, Chittagong