Cybersicherheit in Europa
Prof. Udo Helmbrecht, Geschäftsführender Direktor der ENISA im Experteninterview

Cyber security in Europe
An expert interview with Prof. Udo Helmbrecht, Executive Director of ENISA

Die European Union Agency for Network and Information Security (ENISA) ist ein Kompetenzzentrum für Cybersecurity in Europa. Von ihrem Hauptsitz in Griechenland aus trägt sie zu mehr Netzwerk-und Informationssicherheit in der Europäischen Union bei und fördert die Weiterentwicklung der Awareness und der Sicherheitskultur in der europäischen Gesellschaft.

Der Geschäftsführende Direktor Prof. Udo Helmbrecht ist seit 2009 im Dienste der ENISA. Der Deutsche war vorher Präsident des Bundesamts für Sicherheit in der Informationstechnik – kurz BSI. Vorab begleitete der promovierte Physiker mehrere Ämter in der Privatwirtschaft. Seit 2010 hat er eine Honorarprofessur an der Universität der Bundeswehr inne. Er gibt uns einen Einblick in die aktuellen Themen seiner Institution.

Herr Prof. Helmbrecht, welche Bedeutung hat das Thema Cybersicherheit für die EU-Spitzen?

Die Bedeutung ist stark gewachsen. Natürlich gibt es viele drängende Themen aus verschiedenen Politikbereichen auf der Agenda der Kommissare. Aber man merkt, dass das Thema Cybersicherheit sehr ernst genommen wird und der Wille da ist, Europa umfassend zu schützen. EU-DSGVO, NIS Direktive, Cybersecurity Act oder EU Cyber Diplomacy Toolbox sind einige Beispiele, die zeigen, dass die Bemühungen in eine weitreichende Gesetzgebung und umfassende Maßnahmen münden.

Wie unterstützt die ENISA dabei, Europa sicherer zu machen?

Einerseits unterstützen wir Mitgliedsstaaten bei der Umsetzung der Vorgaben der EU. Besonders kleine Staaten stehen hierbei im Fokus. Andererseits sind wir auch Ideengeber oder Gesprächspartner wenn es darum geht, Technologien zu identifizieren, die in fünf oder mehr Jahren so wichtig sind, dass sie auf der europäischen Ebene reguliert werden sollten. Vor circa acht Jahren war Cloud Computing so ein Thema. Und man sieht heute,

The European Union Agency for Network and Information Security (ENISA) is a competence centre for cybersecurity in Europe. From its headquarters in Greece, it contributes to improving network and information security in the European Union and promotes the further development of awareness and the security culture in European society.

Executive Director Prof. Udo Helmbrecht has been working for ENISA since 2009. The German national was previously President of the Federal Office for Security in Information Technology – BSI for short. Previously, the PhD physicist occupied several positions in the private sector and, since 2010, he holds an honorary professorship at Bundeswehr University. He gives us an insight into the current topics of his institution.

Prof. Helmbrecht, what is the importance of cyber security for EU leaders?

Its significance has grown immensely. There are naturally many pressing issues from different policy areas on the agenda of the commissioners. However, it is clear that cybersecurity is taken very seriously and that there is a desire to protect Europe in a comprehensive way. The EU GDPR, NIS Directive, Cybersecurity Act or EU Cyber Diplomacy Toolbox are some examples that show that such efforts lead to far-reaching legislation and comprehensive action.

How does ENISA help to make Europe safer?

On the one hand, we help Member States with the implementation of EU regulations. A particular focus here is on small countries. On the other hand, we are also the source of ideas or dialogue when it comes to identifying technologies that will be so important in five or more years that they should be regulated at the European level. About eight years ago, cloud computing was such an issue. And you can see today how important it

welche Bedeutung es in der Praxis bekommen hat. Heute drehen sich die Diskussionen zum Beispiel um Blockchain oder Quantum Computing. Ein weiterer Schwerpunkt unserer Tätigkeiten ist speziell auf kritische Infrastrukturen und strategisch wichtige Themen ausgerichtet. Eine große Herausforderung speziell im Gesundheitsbereich ist eine Initiative, die wir aktiv begleiten. Andererseits ist auch der Expertenmangel ein Thema, bei dem wir beratend agieren. Zum Beispiel wenn es darum geht, zu definieren wer heute und zukünftig auf EU-Ebene genau gesucht wird. Wir können niemanden „klonen“ und müssen uns bewusst sein, dass es mehrere Generationen dauern kann, bis wir die benötigte Zahl an Experten ausgebildet haben.

Die EU-DSGVO findet seit einigen Monaten in allen EU-Staaten Anwendung. Wie verlief diese Zeit aus Ihrer Sicht?

Es ist noch zu früh für abschließende Schlussfolgerungen. Aufgefallen ist, dass es zwar einige Unternehmen gab, die sich frühzeitig auf das Startdatum vorbereiteten. Aber viele Firmen begannen ihre Aktivitäten „auf den letzten Drücker“. Sie setzten sich erst im Frühjahr mit der neuen Gesetzgebung auseinander. Insgesamt war und ist es für mich aber sehr positiv, zu sehen, dass die Aufmerksamkeit für das Thema Datenschutz und damit auch für die IT-Sicherheit stark gestiegen ist. Wir hatten ja schon vor der EU-DSGVO Datenschutzgesetze, entsprechende Prozesse und Zuständigkeiten in Unternehmen ebenso wie in Behörden. Aber seit Mai 2018 hat das Thema nochmals deutlich an Fahrt aufgenommen. Es wird sehr viel getan. Auch die staatlichen Governancestrukturen in den Mitgliedsstaaten wurden geschaffen oder ausgebaut. Wer die Ansprechpartner in den verschiedenen Ländern sind, ist heute wesentlich klarer. Positiv ist auch, dass die Gesetzgebung international wahrgenommen wird. Die Entwicklung der „Abmahnanwälte“ sorgt mich hingegen. Die Problematik kann vor allem für kleine Unternehmen zu Schwierigkeiten führen.

Herr Prof. Helmbrecht, haben wir derzeit goldene Zeiten für Hacker?

Wenn man die Goldgräberstimmung im Wilden Westen mit dem Aufkommen der neuen Geschäftsmodelle wie Blockchain und Ähnlichem vergleicht, könnte man das so sehen. Kriminelle waren und sind immer da. Sie nutzen heute das Internet und führen teilweise sogar durch von Staaten unterstützte Angriffe durch. Gleichzeitig bauen Institutionen wie die Polizei wesentlich mehr Fachkräfte auf und Europol hat das Cybercrime Centre etabliert. Die Politik investiert also. Ebenso die Unternehmen. Die Investitionen in Prävention und Reaktion steigen und somit die effektive Gegenwehr zu Angriffen.

has become in the real world. Today, the discussions revolve around blockchain, or quantum computing. Another focus of our activities is specifically concentrated on critical infrastructure and strategically important topics. A major challenge focusing particularly on the healthcare sector is an initiative that we actively support. On the other hand, the lack of experts is an issue in which we act in an advisory capacity. For example, when it comes to defining who will be required today and in the future at the EU level. We cannot “clone” anyone, and we need to be aware that it may take several generations to train the required number of experts.

The EU GDPR has been in force for several months in all EU countries. How has this been from your perspective?

It is too early to draw any final conclusions. It was noticeable that, although there were some companies that prepared themselves early for the start date, many companies waited until “the last minute”. They did not take a closer look at the new legislation until the spring. All in all, it has been and is very positive for me to see that the focus on data protection and IT security has increased sharply. We already had, even before the EU GDPR, data protection laws, corresponding processes and responsibilities in companies as well as in public authorities. However, since May 2018, the topic has gained momentum again. There is a lot going on. State governance structures in the Member States were also created or expanded. It is much easier to see today who the contact persons are in the different countries. Another positive factor is that the legislation is receiving international attention. In contrast, the development of “warning lawyers” worries me. This problem can lead to difficulties, especially for small businesses.

Prof. Helmbrecht, are we currently living in a golden age for hackers?

If you compare the gold rush mood in the Wild West with the advent of new business models such as blockchain and the like, you could see it that way. Criminals are and have always been around. Today, they make use of the internet and sometimes even carry out state-sponsored attacks. At the same time, institutions such as the police are substantially increasing their pool of experts and Europol has established the Cybercrime Centre. Governments are thus investing. And so are companies. The level of investment in prevention and response are increasing, thereby improving abilities to fend off attacks.