LEBEN WIR IN GOLDENEN ZEITEN FÜR HACKER?
Statements von Fachexperten

DO WE LIVE IN A GOLDEN AGE FOR HACKERS? – Statements from IT experts

MATHIAS MAIERHOFER, Vorsitzender der Geschäftsleitung bei FL1 – Telecom Liechtenstein
Chairman of the Executive Board at FL1 – Telecom Liechtenstein

Ja, es sind goldene Zeiten für Hacker. In den meisten Unternehmen herrscht noch zu wenig Bewusstsein für das Risikopotenzial und mögliche Angriffsvektoren und man bietet somit insgesamt grosse Angriffsflächen. Diese Umstände spielen Hackern natürlich in die Hände.

Dabei wird es auch für Behörden und Unternehmen immer schwieriger, sich durch eigenes Know-how zu schützen und Angriffe zeitnah als solche erkennen zu können. Personal mit der nötigen Ausbildung und Erfahrung ist knapp, die eingesetzten Tools für Abwehr sowie Erkennung werden stets komplexer und die notwendigen Prozesse für eine schnelle Reaktion auf einen Angriff sind oft nicht in ausreichendem Masse vorhanden. Wie lange wir daher noch in einem goldenen Zeitalter für Hacker leben, hängt stark von der Bereitschaft von Unternehmen und Behörden ab, sich rascher gegen Cyberangriffe fit zu machen.

Yes, these are golden times for hackers. In most companies there is still too little awareness of the risk potential and possible attack vectors thus a lot of targets for them to attack. Of course, these factors play into the hands of hackers.

At the same time, it is becoming increasingly difficult for authorities and companies to protect themselves with their own know-how and to detect attacks in a timely manner. Staff with the necessary training and experience is scarce, the tools used for defence and detection are becoming increasingly complex and processes for a quick response to an attack are often not sufficiently established. How much longer we will live in golden times for hackers heavily depends on the willingness of companies and authorities to make themselves fit to ward off cyber attacks.

HENDRIK F. LÖFFLER, Mitglied der Geschäftsleitung der Funk Gruppe
Member of the Executive Board of Funk Gruppe

Zunehmend erleben wir in Unternehmen eine Sensibilisierung für das Thema Hacking. Insofern haben es Hacker heute nicht mehr ganz so leicht; aber auch die Cyberkriminellen entwickeln sich weiter! Alleine in den letzten Monaten haben wir über 60 Workshops zur Risikobewertung durchgeführt und mit unseren Mandanten an der Optimierung ihrer Risikomanagementstrategie gearbeitet. Viele Unternehmen bewerten Angriffe von außerhalb nun deutlich realistischer als zuvor, vergessen dabei aber gerne, dass der Ausfall oder die Schädigung der Unternehmens-IT auch von innen erfolgen kann. Hier sehen wir deutlichen Nachholbedarf!

We are experiencing an increase of awareness for the topic of hacking in companies. In this respect hackers no longer have it that easy, but cybercriminals are refining their techniques as well! In recent months alone, we have conducted over 60 workshops to assess risks and have worked with our clients to optimise their risk management strategies. Many companies now evaluate attacks from the outside much more realistically than before but tend to forget that the failure or damage of their company's IT can also happen from within. We see a clear need to catch up!

ANDREAS BECHTOLD, Geschäftsführer Infinigate Deutschland GmbH
Managing Director Infinigate Deutschland GmbH

Um IT-Umgebung im Unternehmen vor modernen Hackerangriffen zu schützen, ist eine permanente Überwachung, Analyse und Risikobewertung unabdingbar.

Mit einer SOC as a Service Lösung fällt der enorme Aufwand für den Betrieb eines eigenen Security Operation Centres weg und Unternehmen können sich somit primär auf das Wesentliche, also die Beseitigung von Schwachstellen, konzentrieren.

Permanent monitoring, analysis and risk assessment are indispensable in order to protect companies' IT environments against modern cyber attacks.

With a SOC as a Service solution, the enormous expense of operating a Security Operations Centre is eliminated, allowing companies to concentrate primarily on the essentials, i.e. eliminating weak points.

FRANK HEINZMANN, Vorstandsmitglied bei der Information Security Society Switzerland (ISSS)
Member of the Board, Information Security Society Switzerland (ISSS)

Meines Erachtens gab es die "Goldenen Zeiten" für den typischen "Hacktivist" auch bereits in der Vergangenheit. Das einfachste Ziel war, ist und werden meiner Meinung nach auch in der nahen Zukunft immer noch Endbenutzer und KMUs bleiben, also die breite Masse, der es an Know-how und Mitteln für adäquaten Schutz fehlt.

Allerdings haben sich die Akteure und die Angriffsvektoren verschoben, und wenn wir vom "typischen" Hacker zu organisierten oder Staaten-gestützten Cyberattacken und –terror übergehen, sieht die Situation ganz anders aus. Dort werden hoch-spezialisierte, komplexe Attacken gegen ausgewählte Objekte mit ganz konkreten Zielsetzungen gefahren. Für diese steht in der Regel viel Geld zur Verfügung – und ja, in diesem Zusammenhang könnte man von "Goldenen Zeiten" für die Akteure sprechen.

In my point of view, there was already a 'golden age' for the typical 'hacktivist' in the past. The easiest target was, is and, in my opinion, will remain in the near future end users and SMEs, i.e. the broad population that lacks the know-how and resources to ensure appropriate levels of protection.

However, the protagonists and the attack vectors have shifted, and when we move from 'typical' hackers to organised or state-supported cyber attacks and terror, the situation is very different. There, highly specialised, complex attacks are launched against selected targets with very specific objectives. As a rule, substantial funds are available for these – and yes, in this context, one could speak of a 'golden age' for the players involved here.

HASSAN MARZOUK, Head of Sales DACH bei RadarServices
Head of Sales DACH at RadarServices

Es sind wahrlich goldene Zeiten für Hacker. Viele Unternehmen und Behörden sind unzureichend auf die heutigen Herausforderungen vorbereitet. Das öffnet Cyberangreifern Tür und Tor. Mittlerweile muss jede Organisation davon ausgehen, Ziel von Angriffen zu werden. Wer sich nach dem Motto „mich wird es schon nicht treffen" in falscher Sicherheit wiegt anstatt entsprechende Vorkehrungen zu treffen, riskiert massiven Schaden für seine Organisation, die Beschäftigten, die Kunden, die Lieferanten und alle anderen Stakeholder. Die goldenen Zeiten für Hacker können nur eingedämmt werden, wenn Unternehmen und Behörden den Handlungsbedarf rasch erkennen und adäquat auf die tatsächlichen Risiken reagieren. Dann wird das „Geschäftsmodell Hacking" weniger lukrativ und damit uninteressanter für die, die es betreiben.

These are truly golden times for hackers. Many companies and authorities are inadequately prepared for today's challenges. This fact opens up a lot of possibilities for cyber attackers. Every organization must consider the fact that it will become the target of attacks. Those who lull themselves into a false sense of security, thinking "I won't be the next victim", instead of taking the appropriate precautions, risk massive damage to their organisation, employees, customers, suppliers and other stakeholders. The golden times for hackers will only come to an end if companies and authorities quickly recognize the need for action and react adequately to the actual risks. Then the "hacking as a business model" becomes less lucrative and less interesting for those who run it.

PROF. DR. PAVEL LASKOV, Hilti Lehrstuhl für Daten- und Anwendungssicherheit, Universität Liechtenstein, Institut für Wirtschaftsinformatik
Hilti Chair for Data and Application Security, University of Liechtenstein, Institute of Information Systems

Ja, absolut. Je mehr wir kritische Aufgaben unseres Lebens auf Computergeräte „auslagern", desto sinnvoller ist es für Kriminelle diese zu hacken. Wer Lösegeld zahlt, um einen verschlüsselten Laptop oder ein Handy zu retten, wird dies sicherlich auch tun, um die "kaputten" Autobremsen zu "reparieren", den Zutritt zu seinem Haus zu öffnen oder den Herzschrittmacher wieder einzuschalten. Alle begehrten und äußerst nützlichen Funktionen, die uns durch neuartige IT-Technologien zur Verfügung gestellt werden, erhöhen ihre Komplexität und zwangsläufig die Angriffsfläche. Das sind hervorragende Nachrichten für Hacker, um damit ihren Lebensunterhalt und etwas mehr zu verdienen.

Yes, absolutely. The more critical tasks of our life we "outsource" to computing devices, the more it makes sense for criminals to hack them. Whoever pays ransom to salvage an encrypted laptop or mobile phone, will certainly do so for "repairing" the "broken" car brakes, opening the door to his home or turning his heart pacemaker back on. All of the coveted and, indeed, extremely beneficial features brought to us by novel IT technologies increase their complexity and, necessarily, the attack surface. Excellent news for the hackers to earn their living and a bit more.