carmasec

security. done. right.

Interview mit Prof. Dr. Norbert Pohlmann

Professor für Informationssicherheit
Institutsleiter für Internet-Sicherheit
Pionier der Cybersicherheit

In unserer Interviewreihe stellen wir Ihnen Persönlichkeiten vor, die sich in der Cybersicherheits-Forschung verdient gemacht haben.

Wir haben mit Prof. Dr. Norbert Pohlmann, Professor für Internetsicherheit und Pionier der Cybersicherheit, darüber gesprochen, welchen Beitrag die Wissenschaft zum Schutz der Gesellschaft leisten kann und muss.

1. Sie sind bereits langjährig in ganz unterschiedlichen Rollen im Bereich Cybersicherheit aktiv: als Hochschulprofessor und Institutsleiter, Verbandsaktivist, Mitglied in Expertenausschüssen, Investor bei Cybersecurity-Startups, Buchautor und zuvor auch in der Unternehmensführung verschiedener Hersteller von IT-Sicherheitslösungen. In welcher Rolle haben Sie den Eindruck, am meisten Wirkung im Themenbereich Cybersicherheit zu haben, oder ist es die Kombination der verschiedenen Funktionen?


Prof. Dr. Norbert Pohlmann

In allen meinen Rollen habe ich immer eine Wirkung auf den Themenbereich Cyber-Sicherheit ausüben können. Dennoch hat jede Rolle auch verschiedene Möglichkeiten. In der Zeit als Unternehmer habe ich gelernt, sehr präzise Ziele zu definieren und diese dann erfolgreich umzusetzen. Als Professor habe ich immer wieder die Gelegenheit, mich neu zu erfinden und mit den Studierenden Sachthemen zu diskutieren. Als Forscher kann ich Innovationen nachgehen und immer schon die nächste Generation von Cyber-Sicherheitslösungen denken und umsetzen. Mein Engagement in den Verbänden gibt mir die Möglichkeit, die Realitäten der Firmen mit den Ideen der Hochschule zusammenzubringen und den geschützten Raum des Elfenbeinturms zu verlassen, aber auch besonders den Cyber-Sicherheitsmarkt mit zu gestalten.

Die Startups helfen, den Technologietransfer aus der Hochschule in die Wirtschaft zu beschleunigen und damit sehr gute Cyber-Sicherheitslösungen schnell für mehr Sicherheit umzusetzen. Fachbücher zu schreiben, ermöglicht es, meine Ideen und meine Erfahrungen einer breiteren Masse zur Verfügung zu stellen. Heute kann ich die Erfahrungen aus den unterschiedlichen Bereichen nutzen, um meine gewollte Wirkung zu optimieren.

2. Sie waren früher selbst Geschäftsführer eines Hersteller von Verschlüsselungslösungen und fordern in Ihren Vorträgen häufig eine stärkere Produkthaftung der Hersteller bei unsicher entwickelten Produkten. Wie schätzen Sie die Chancen ein, dass dies mit den jüngsten regulatorischen Anforderungen (IT-Sicherheitsgesetz, Datenschutzgrundverordnung, u.a.) ein erster wirksamer Schritt sein kann? Und sehen Sie hier realistische Möglichkeiten für einen internationalen, standardisierten Ansatz?

Ja, als Unternehmer habe ich gelernt, dass der Kunde sich auf unsere IT-Sicherheitslösungen verlassen muss! Daher haben wir immer schon die Verantwortung übernommen. In vielen Bereichen der IT ist das anders. Aber aus meiner langjährigen Erfahrung kann die Produkthaftung die Firmen motivieren, ihre Produkte sicher und vertrauenswürdig zu entwickeln. Nur so habe wir gemeinsam ein Chance, die Digitalisierung erfolgreich und nachhaltig umzusetzen. Mit dem europäischen Datenschutzgesetz und den daraus folgenden hohen Strafen bei Zuwiderhandlung haben wir erreicht, dass weltweit die Unternehmen heute unsere ethischen Vorstellung von Datenschutz umsetzen müssen!

3. Wie bewerten Sie die jüngst veröffentlichten Hintergrundinformationen bei der Schweizer Crypto AG und dem Einfluss von in- und ausländischen Nachrichtendiensten. Missbrauchen wir hierdurch nicht das grundsätzliche Vertrauen der Anwender in Verschlüsselungsmechanismen und verlieren wir damit nicht ein wesentliches und wirksames Instrument im Kampf gegen Cyberangriffe?

Ja, genau so ist das! Wenn der Staat seine Interessen höher bewertet als die der Bürger, baut das kein Vertrauen auf, sondern genau das Gegenteil.

Dass die Crypto AG im Einfluss in- und ausländischer Nachrichtendienste steht, hat jeder gewusst! Am Ende ist es für alle ein bekannter und abgesprochener Deal! USA, Deutschland und andere „verkaufen“ im Rahmen der Entwicklungshilfe Crypto-Geräte in Länder, bei denen sie alles mitlesen können. Die Länder, die diese Geräte nutzen, wissen das, können sich damit aber gegen den Rest der Welt schützen (Russland, China etc.). Daher sollten wir eine solche Praxis nicht tolerieren und entsprechende politische Konsequenzen daraus ziehen!

4. Cyberangriffe treffen zunehmend mehr privat-wirtschaftliche Unternehmen aber auch öffentliche Institutionen und Organisationen. Häufig kommen diese Angriffe vermeintlich von Hackergruppen, die von ausländischen Geheimdiensten unterstützt sein könnten. In diesem Zusammenhang werden Rufe nach einem „Hackback“ oder „Cyber-Gegenangriffen“ laut. Wie schätzen Sie die Sinnhaftigkeit und Wirksamkeit dieser Gegenschläge ein?

Am wichtigsten ist es, sich mit Hilfe der Cyber-Sicherheitsstrategien zur Reduzierung von Risiken zu schützen. Das sind „Vermeidung von Angriffen“, wie beispielsweise keine Technologien mit Schwachstellen zu nutzen oder sich auf die wichtigsten Werte und IT-Systeme zu konzentrieren. Weiterhin ist das „Entgegenwirken gegen Angriffe“ durch starke Authentifikation, Verschlüsselung, Firewall, Anti-Malware, usw. relevant. Da auch diese Cyber-Sicherheitsstrategien zu Reduzierung von Risiken keine 100-prozentige Cyber-Sicherheit garantieren können, müssen wir mit verbleibenden Risiken rechnen. Die Sicherheitsstrategien, die hier helfen, sind zum einen das „Erkennen von Angriffen“ - mit Cyber-Sicherheitsfrühwarnsystemen Angriffe so schnell wir mögliche zu erkennen - und zum anderen das „Reagieren auf Angriffe“, wenn diese erkannt wurden, um Schäden zu vermeiden oder zumindest zu reduzieren.

Wenn ein „Hackback“ oder „Cyber-Gegenangriff“ hilft, einen Schaden zu verhindern oder zu reduzieren, sollte er auch von Profis umgesetzt werden. Wichtig ist nur, dass die Konsequenzen und Risiken vorher klar beschrieben und das Konzept des Gegenangriffes von kompetenten Cyber-Sicherheitsexperten getestet worden ist und der eigentliche Gegenangriff protokolliert wird.

5. Die Digitalisierung erreicht immer mehr Lebensbereiche und bietet an vielen Stellen enormes Potential, um den Lebensstandard und -komfort für viele Menschen weiter zu erhöhen. Unternehmen sehen durch die Digitale Transformationen die Chance für neue Geschäftsmodelle oder höhere Produktivität beispielsweise durch Automatisierung. Ausgeblendet werden sowohl im privaten als auch im geschäftlichen Einsatz allerdings oft die damit verbundenen Risiken — verlieren wir endgültig die Kontrolle über die eingesetzte Technologie?

Ja, das ist ein Dilemma! Auf der einen Seite werden wir für das Wohl unserer Gesellschaft nicht auf die Digitalisierung verzichten können. Auf der anderen Seite müssen wir erkennen, dass die Risiken der IT jedes Jahr steigen!

Aus diesem Grund müssen alle Stakeholder zusammenarbeiten und gemeinsam mit guten Zielen und Vorgehensweisen dafür sorgen, dass wir perspektivisch deutlich mehr Cyber-Sicherheitsmechanismen einsetzen und damit das Risiko für unsere Zukunft in diesem Bereich immer mehr reduzieren.

6. Gerade bei mittelständischen Unternehmen oder Organisationen in IT-fernen Branchen ist das Bewusstsein der Unternehmensführung für Cybersicherheit häufig immer noch niedrig und der Reifegrad der implementierten Sicherheitsmechanismen schlecht, obwohl bezahlbare Lösungen längst am Markt verfügbar sind und gegen viele Bedrohungen einen wirksamen Schutz bieten würden. Was haben wir in der Branche in den letzten Jahren falsch gemacht?

Die Marktführer im Bereich der IT kommen aus den US und Asien. In diesen Ländern wird das Thema Cyber-Sicherheit nicht mit der gleichen Priorität betrachtet, wie bei uns. Daher müssen die Unternehmen in der Regel zusätzlich Cyber-Sicherheitslösungen einsetzen. Diese sind in der Regel für den normalen Nutzer auch noch schwierig zu bedienen und machen die eigentliche Arbeit komplizierter. Wir müssen es in Zukunft schaffen, dass die notwenige IT, die sich im Rahmen der Digitalisierung sowieso ändert, mit Cyber-Sicherheitsarchitekturen und -mechanismen ausgestattet wird, die eine deutliche höhere Wirkung gegen Angriffe erzielen, am besten ohne die Einwirkung der Nutzer funktionieren und eine hohe Qualität besitzen.

7. Bei privaten Anwendern setzen sich neue Technologien im Regelfall deutlich schneller durch als im Unternehmenseinsatz, nach dem Smartphone und Tablet kommen nun immer mehr Geräte ins „Smart Home“. Während der Nutzwert und der Komfort der neuen Produkte den Nerv der Zielgruppe offenbar treffen, scheint das technische Verständnis über die Funktionsweise und das Wissen ums die Missbrauchsmöglichkeiten bei den Anwendern zu sinken. Was können wir hier im Bildungssystem unternehmen, um hier gerade Privatanwender besser über die Risiken aufzuklären?

Wir sollten den Nutzer nicht mehr als das schwächste Glied in der Cyber-Sicherheit betrachten. Bei Sicherheitsvorfällen dem Nutzer die Schuld zuzuweisen, ist keine zielführende Cyber-Sicherheitsstrategie. Wir sollten die IT-Technologie analysieren, wenn Nutzer-Fehler zu Sicherheitsproblemen führen. Denn wenn Nutzer sich nicht an Sicherheitsregeln halten, liegt dies meist daran, dass es oft zeitraubend oder schwierig bis unmöglich ist, sie umzusetzen. Wir brauchen bessere technische IT-Lösungen, die im Gebrauch einfach sind. Ziel muss es sein, die IT-Technologie an den Menschen anzupassen, um diesen zu entlasten und zu schützen.

8. Was kann der akademische Bereich tun, um eine Immunisierung der Gesellschaft gegen Cyberangriffe zu fördern? Was wären Ihre Ansatzpunkte?

IT-Systeme müssen in der Zukunft angriffsresilienter werden. Die IT-Systeme der Zukunft müssen so konzipiert und umgesetzt werden, dass sie in der Lage sind, kompromittierte Systemteile zu tolerieren. Die IT-Systeme müssen auch dann noch verlässlich arbeiten, wenn sie von Angreifern attackiert werden. Dazu brauchen wir Mindestsicherheitsstandards für IT-Systeme, die mit Hilfe von Anreizsystemen Unternehmen motivieren, um einen flächendeckenden Einsatz zu erreichen.

9. Sie sind auch als Förderer von Startups im Bereich der Cybersicherheit aktiv, u.a. auch bei XignSys und AWARE7 sowie bei einigen anderen Jungunternehmen, deren Gründer zuvor Studenten an Ihrem Institut für Internet-Sicherheit an der Westfälischen Hochschule waren. Wie schätzen Sie das Potential Ihrer Studenten hierzulande - im Vergleich zu den im Security-Bereich weiterhin führenden Ländern USA und Israel - ein? Wo und wie müssen wir uns noch verbessern, damit wir ähnlich erfolgreiche Ökosysteme für Unternehmensgründer in diesem Bereich hier in Deutschland schaffen können?

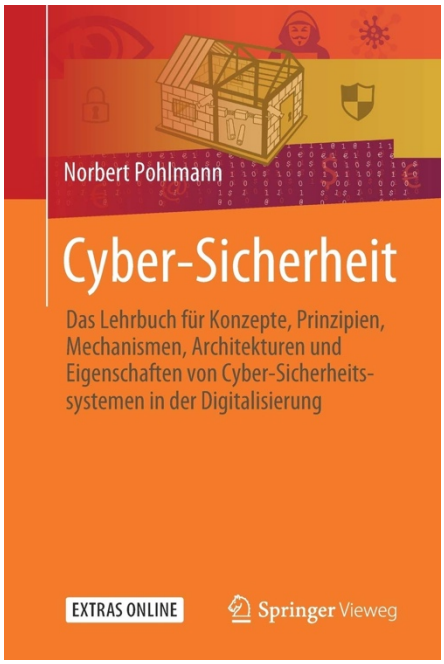
Die Absolventen im Bereich Informatik an der Westfälischen Hochschule sind sehr gut ausgebildet, leistungsfähig und bereit, ihren Beitrag für die Zukunft engagiert zu erbringen.
Wenn sie dann noch einige Zeit im Institut für Internet-Sicherheit geforscht haben, sind sie in der Lage, die notwendigen Innovationen im Bereich der Cyber-Sicherheit umzusetzen und diese als nutzbare IT-Systeme für den Markt zu erstellen. Der Technologietransfer von Hochschule in die Wirtschaft mit Hilfe der Startups funktioniert am schnellsten und besten.

Auf der fachlichen Cyber-Sicherheitsebene sind wir allen anderen Ländern mehr als ebenbürtig.
Die Herausforderungen in Deutschland liegen im Hochschulbereich in der frühen Motivation der Studierenden, wie zum Beispiel anrechenbare Fächer im Bereich „Entrepreneur“ „Vertrieb“, „Marketing“, usw. sowie Matching von Studierenden verschiedener Disziplinen, die für ein erfolgreiches Startup notwendig sind. Im Bereich der Wirtschaft haben wir einen großen Nachholbedarf an Anerkennung der Leistung der Startups und deren Gründer sowie die Möglichkeiten der Zusammenarbeit der Startups mit der Wirtschaft.

10. Bei dem ständig steigenden Innovationstempo der technischen Entwicklung, wo sehen Sie die Cybersicherheit in den nächsten 5 bis 10 Jahren? Haben wir eine realistische Chance den Kampf gegen professionalisierte Cyberangreifer zu gewinnen oder werden wir bis dahin längst von unserer eigenen Version von 'Skynet' kontrolliert?

Im Prinzip haben wir alle Voraussetzungen, den Kampf gegen professionalisierte Cyberangreifer zu gewinnen. Wir müssen nur mit allen Stakeholdern zusammen die richtigen Ziele definieren und anschließend gemeinsam umsetzen!

Klar ist, ohne Cyber-Sicherheit wird keine nachhaltige Digitalisierung funktionieren.
Wir sind also zum Erfolg verdonnert!



Prof. Dr. Pohlmann ist Autor des Standard-Werkes "Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung"; dass im Springer-Vieweg Verlag in Wiesbaden 2019 in seiner aktuellen Auflage erschienen ist.