PAUSENLOSE FEINDBERÜHRUNG. DIE CYBERVERTEIDIGUNG DER POLNISCHEN ARMEE

Im Kampf gegen russische und weißrussische Eindringlinge.

Ein Gespräch mit Brigadegeneral Karol Molenda, dem Kommandeur des Nationalen Zentrums für Cybersicherheit (NCBC).

Brigadegeneral Karol Molenda, Jahrgang 1980, ist seit Februar 2019 Bevollmächtigter des Verteidigungsministeriums für den Aufbau der Cyber-Verteidigungstruppen. Sie sollen bis Ende 2024 ihre volle Kampfkraft erreichen und ab dann als die sechste Teilstreitkraft der polnischen Armee fungieren, neben dem Heer, der Luftwaffe, der Marine, den Spezialtruppen und der Territorialverteidigung. Zum Brigadegeneral (es ist der unterste der vier Generalsränge) wurde Molenda im März 2019 befördert.

Er ist Absolvent der Warschauer Technischen Militärakademie (Master-Abschluss als Ingenieur an der Elektronik-Fakultät und postgraduales MBA-Studium an der Fakultät für Kybernetik auf dem Gebiet der Cybersicherheit) sowie der Hochschule für Management in Warschau.

Molenda gilt als ein geborenes Organisationstalent und genießt zugleich den Ruf eines hervorragenden IT-Analytikers. Zwischen 2007 und

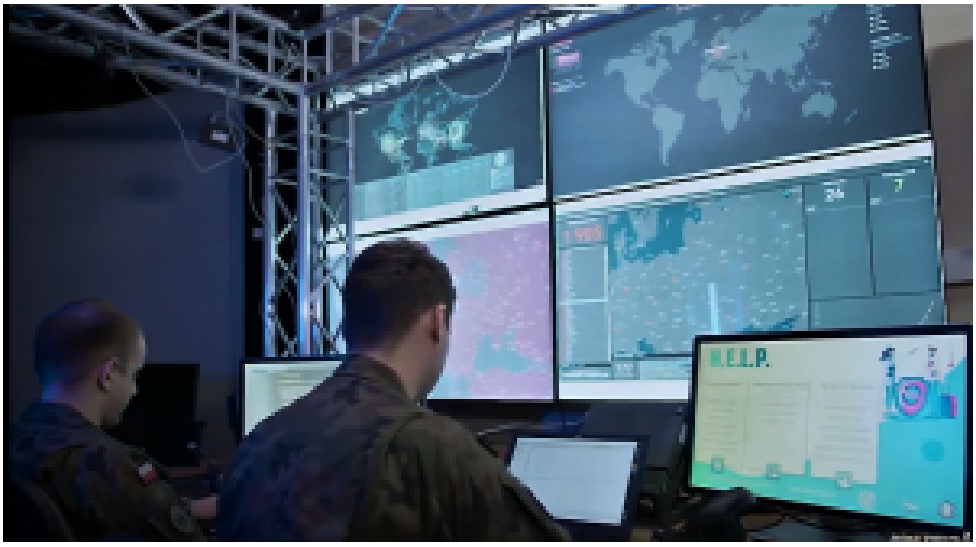
2019 war er beim Militärischen Abschirmdienst tätig, wo er zuletzt die Abteilung für Cyber-Spionageabwehr leitete.

General Molenda im Serverraum, dem Herzstück des Nationalen Zentrums für Cybersicherheit (NCBC) in Legionowo bei Warschau.

Er gibt zu, dass er sich schon immer sehr für Informations- und Kommunikationssicherheit interessiert hat. „Ich habe mich mit allem befasst, was Systeme zur Verarbeitung von Verschlusssachen angeht: Zertifizierung von Geräten und Verfahren, die zum Schutz eingesetzt werden, IKT-Sicherheitsakkreditierung, Härtung und Audits von IKT-Systemen und deren Überwachung“.

Molenda gilt als Experte für das Reagieren auf Computerzwischenfälle, für Computerforensik und die gezielte Suche nach Bedrohungen. Er war maßgeblich beteiligt an der Einrichtung eines der technisch fortschrittlichsten Labore für Computerforensik in Polen und wahrscheinlich in ganz Europa.

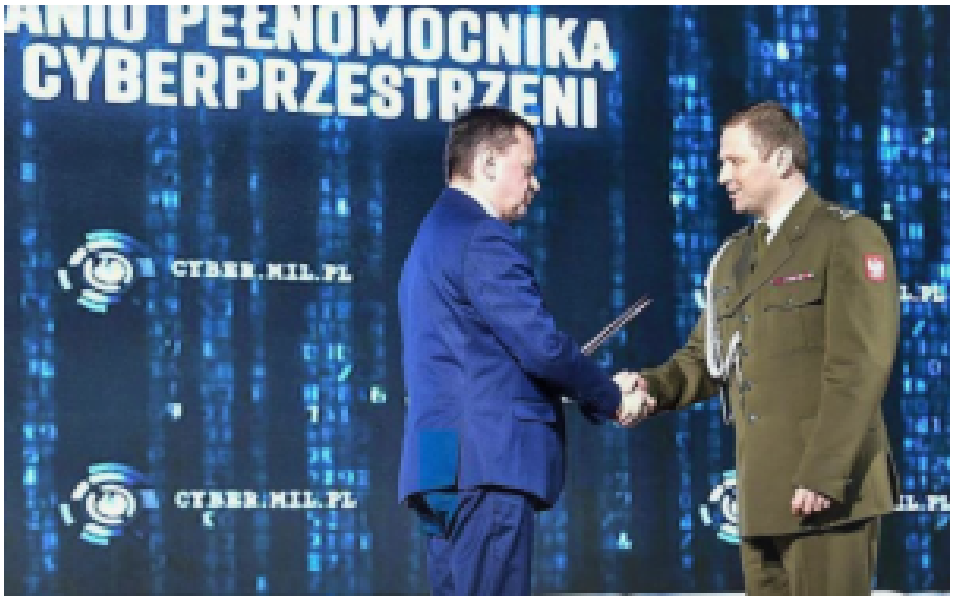
Seit Februar 2019 leitet Molenda das Nationale Zentrum für Cybersicherheit (NCBC). Es hat seinen Sitz auf einem streng abgeschirmten Gelände in Legionowo, einer Kleinstadt vor den Toren Warschaus. Von dort aus werden rund um die Uhr die gesamten Online-Aktivitäten der polnischen Armee überwacht, abgeschirmt und Cyberattacken abgewehrt.



Lageraum des Nationalen Zentrums für Cybersicherheit.

Frage: Im vor uns liegenden Jahr wird das Nationale Zentrum für Cybersicherheit drei Jahre alt. Wie stark hat die Bedrohung durch Cyberangriffe auf das polnische Militär und seine Einrichtungen in dieser Zeit zugenommen?

Wir haben hart gearbeitet, um die damit verbundenen Risiken so klein wie möglich zu halten. Noch vor wenigen Jahren war das Nationale Kryptologiezentrum für die Cybersicherheit in der Armee zuständig, und die Funktionsfähigkeit der militärischen Systeme wurde von der IT-Inspektion gewährleistet. Es handelte sich um zwei separate Einheiten mit unterschiedlichen Zielen, da ein System nicht gleichzeitig sicher sein und alle vom Nutzer erwarteten Funktionen bieten kann.



Februar 2019. Verteidigungsminister Mariusz Błaszczak beruft (da-

mals noch) Oberst Karol Molenda zum Bevollmächtigten des Verteidigungsministeriums für den Aufbau der Cyber-Verteidigungstruppen.

Vor drei Jahren wurden die beiden Einrichtungen im NCBC zusammengeführt. Wir haben unsere Systeme gestrafft und das Sicherheitsniveau deutlich erhöht, manchmal auch auf Kosten der Funktionsvielfalt. Eine der ersten Maßnahmen war die Einführung von MFA (Multifactor Authentication) für die offizielle Post, d. h. eine mehrstufige Nutzer-Identifizierung, die zuvor weder im Verteidigungsministerium noch bei den Streitkräften Standard war.

Darüber hinaus haben wir die Systeme so eingestellt, dass eine Anmeldung ausschließlich über Dienstgeräte oder spezielle Zugänge (von NCBC entwickelt und installiert) möglich ist. Vieles davon konnte schnell erledigt werden, da das NCBC gleichzeitig Eigentümer aller Computersysteme in der Armee geworden ist.

Wenn also ein System in der Armee nicht mehr funktioniert oder ein Cyberangriff erfolgt, ist das NCBC dafür verantwortlich?

Wir sind das digitale Herz der Armee. Wir sind und fühlen uns für den Betrieb und den Schutz der gesamten militärischen Informations- und Kommunikationstechnik verantwortlich. Nur wir sind berechtigt, sämtliche Sicherheitslösungen in der gesamten militärischen Infrastruktur umzusetzen.

Das Warschauer Kreisgericht verhandelt gegen den ehemaligen Leiter der polnischen Huawei-Niederlassung, dem Spionage vorgeworfen wird und der, nach Angaben der Ermittler, ein verdeckter chinesischer Geheimdienstmitarbeiter war. Die Amerikaner weisen seit langem auf Gefahren hin, die mit dem Einsatz von Systemen und Geräten aus chinesischer Produktion verbunden sind. Verwendet die polnische Armee derartige Produkte?

Wir haben keine chinesische Technologie in unsere militärische Infrastruktur eingebaut. Wir verlassen uns ausschließlich auf die Lösungen unserer NATO-Partner, hauptsächlich aus den Vereinigten Staaten und der Europäischen Union. Auch diese Systeme und Lösungen werden von uns in Bezug auf ihre Sicherheit bewertet, bevor sie bei der Armee eingeführt werden.

„Wir haben keine chinesische Technologie in unsere militärische Infrastruktur eingebaut.“

Wir überprüfen auch alle Systemaktualisierungen. Für sich genommen, enthalten sie vielleicht keine Schwachstellen, aber sobald sie eingebaut sind, könnten sie Pforten öffnen, durch die versucht werden kann, in das System einzudringen. Deswegen bewerten wir vor der Einführung von Aktualisierungen, welche Veränderungen sie in unserem Netz verursachen könnten. Das gilt sowohl für nicht klassifizierte als auch für klassifizierte Systeme. Darüber hinaus unterliegen auch klassifizierte Systeme, gemäß dem Gesetz zum Schutz von Verschlusssachen, einer Sicherheitsakkreditierung, d. h. sie werden von den zuständigen Diensten automatisch auf ihre Sicherheit überprüft.

Chinesische Systeme und Ausrüstung sind für die polnische Armee also inakzeptabel?

China ist weder unser Partner noch ein Verbündeter der NATO oder der Europäischen Union. Außerdem sind chinesische Unternehmen gesetzlich verpflichtet, bestimmte Daten der von ihnen hergestellten Geräte an die dortigen Geheimdienste weiterzugeben. Das birgt erhebliche Gefahren. Deshalb verwenden wir keine chinesische Hardware.

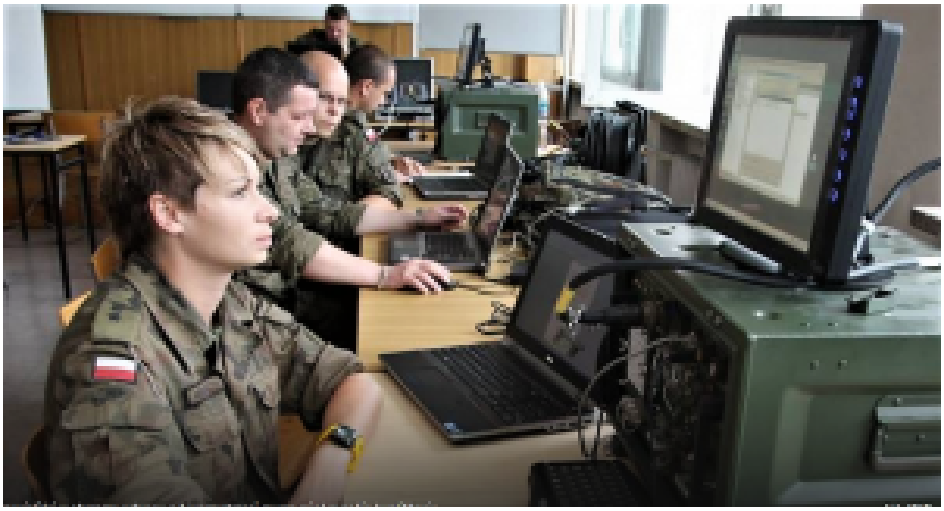
So die aktuelle Praxis. Ich hoffe, dass die Änderung des Gesetzes über das nationale Cybersicherheitssystem uns auch die einwandfreie juristische Handhabe geben wird, die Nutzung nicht vertrauenswürdiger Systeme und Geräte, die eine Bedrohung für die Sicherheit darstellen könnten, vollständig zu blockieren.

Wie werden die private Ausstattung und die privaten E-Mail-Postfächer der Offiziere und der Beamten des Verteidigungsministeriums geschützt?

Kein System kann vollständig vor Missbrauch geschützt werden. Die Amerikaner haben dafür ein gutes Sprichwort: „There is no patch for human stupidity“ – sinngemäß, „Gegen menschliche Dummheit ist kein Kraut gewachsen“.

Daher können wir die Risiken nur durch Schulung und Beratung verringern. Ein Großteil unserer Arbeit besteht deswegen aus eindringlicher Bewusstmachung, wie wichtig Cyberhygiene ist. Das sind gemeinschaftliche Vorsichtsmaßnahmen von Sicherheitsfachleuten, Administratoren und Nutzern, um sich vor Angriffen zu schützen.

Wer sich ausschließlich auf Security-Experten verlässt, übergeht die Rolle, die ein einzelner Mitarbeiter bei der Gewährleistung der Sicherheit spielen kann. Wenn Mitarbeiter und alle Endanwender die grundlegenden Praktiken der IT-Hygiene verstehen, spielen sie eine wichtige Rolle beim Schutz der Geräte und Netzwerke.



„Selbst der elektronische Schriftverkehr zwischen Soldaten findet innerhalb des geschlossenen Systems statt. In den gesamten Streitkräften ist das der elementare Kommunikationskanal, der vollständig überwacht wird“.

Es geht also nicht nur um die ranghöchsten VIP‘s, die die vertraulichsten Geheimnisse des Verteidigungswesens kennen, sondern auch um all die Soldaten und Ministerialbeamten, die Zugang zu den von uns geschützten Netzwerken haben. Um sie alle in Sachen IT-Hygiene auf dem Laufenden zu halten, haben wir das Zentrum für IT-Sicherheitsschulung

eingerichtet. Außerdem dürfen nach den Richtlinien des Verteidigungsministeriums dienstliche Informationen nur in den vom Ministerium verwalteten Systemen verarbeitet werden. Private E-Mail-Postfächer dürfen nur für den Versand privater Informationen genutzt werden.

In der Armee ist es also unmöglich, dienstliche Nachrichten an ein privates E-Mail-Postfach zu senden?

Das klassifizierte System, das u.a. alle Datenbanken umfasst, läuft vollständig separat, wodurch so etwas nicht möglich ist. In offenen Systemen hingegen, werden dienstliche E-Mails speziell gekennzeichnet und überwacht. So wird jede E-Mail, die an ein Postfach außerhalb des Verteidigungsministeriums geht detailliert ausgewertet.

Das ist notwendig, denn schließlich muss sich das Ministerium mit Institutionen außerhalb des Militärs elektronisch austauschen können. Private Postfächer dürfen hierfür jedoch nicht verwendet werden. Das offene militärische IT-System dient somit nur der notwendigen Unterstützung bei Kontakten nach außen. Jede Auffälligkeit bei der Nutzung wird eingehend analysiert, und die zuständige Sicherheitsdienststelle informiert im Zweifelsfall den Militärischen Abschirmdienst.

Selbst der elektronische Schriftverkehr zwischen Soldaten findet innerhalb des geschlossenen Systems statt. In den gesamten Streitkräften ist das der elementare Kommunikationskanal, der vollständig überwacht wird. Es ist nicht möglich, einen privaten, nicht verifizierten Datenträger an das Dienstsystem anzuschließen. So etwas wird sofort erkannt, blockiert und geahndet. Es gibt somit keine Möglichkeit, dass jemand beispielsweise Arbeit mit nach Hause nehmen würde.

Einem Bericht des amerikanischen Cyber-Sicherheitsunternehmens Mandiant zufolge ist Polen in letzter Zeit zu einem der Hauptziele massiver Cyberangriffe geworden. Sie werden von Gruppen durchgeführt, die mit den Geheimdiensten Russlands und Weißrusslands in Verbindung stehen. Können Sie das bestätigen?

Militärische Systeme sind ein gefundenes Fressen für ausgeklügelte, gut strukturierte Hackergruppen, die im Auftrag und Schutz ausländischer Geheimdienste arbeiten. Im Augenblick sind einige von ihnen sehr aktiv. Doch wir warten nicht darauf, bis wir von ihnen angegriffen werden, sondern machen mit Hilfe von Überwachungssystemen Jagd auf sie.

Gegner sind ausgeklügelte, gut strukturierte Hackergruppen, die im Auftrag und Schutz ausländischer Geheimdienste arbeiten.

Wir gehen ständig davon aus, dass sich jemand Zugang zu unserem System verschafft haben könnte. Wir suchen nach jeder Spur einer solchen Tätigkeit. Wir erstellen und aktualisieren Datenbanken über die Taktiken, Techniken und Verfahren, die unsere potenziellen Gegner anwenden. Sobald sich deren Arbeitsweise ändert oder sie ein neues Verfahren anwenden, setzen wir diese als Modell auf unseren Geräten ein, um so die neuartigen Aufklärungs- oder Eindringungsversuche zu erkennen.

Darüber hinaus, und das ist das Wichtigste, haben wir sehr stark in die Sicherheit unserer Netzlösungen investiert. Daher glaube ich, dass die Kosten eines Angriffs derzeit in keinem Verhältnis zu den Ergebnissen stehen würden. Es dürfte sich für einen Angreifer nicht lohnen, so viel Geld zu investieren, um in unser Netz einzudringen und sofort entdeckt zu werden. Daher ist es für solche Gruppen heute leichter, psychologische Operationen durchzuführen. Sie erstellen gefälschte Konten, verbreiten Desinformationen, dringen in private E-Mail-Postfächer ein.

Damit sind wir bei der „E-Mail-Affäre“, d. h. dem Durchsickern von Korrespondenz aus den elektronischen Postfächern der wichtigsten polnischen Beamten. Wie viele Vertreter der Armee und des Verteidigungsministeriums wurden gehackt, in wie viele private E-Mail-Postfächer wurde erfolgreich eingebrochen?

Uns liegen Informationen vor, wonach versucht wurde, auf diese Weise aktive wie auch pensionierte Offiziere anzugreifen. Es waren mehrere Personen. Jede von ihnen ist von uns informiert worden.

Wurden die Postfächer dieser Personen kopiert?

Das ist keine Frage für uns. Wir überwachen keine privaten E-Mail-Postfächer. Das liegt nicht in unserer Zuständigkeit. Für die gesamte Cyber-Spionageabwehr sind die Geheimdienste zuständig: der Militärische Abschirmdienst SKW und der Inlandsgeheimdienst ABW.

Wir können die Betroffenen nur dazu ermutigen, die Regeln der Cyberhygiene auch privat anzuwenden. Wir haben eine spezielle Online-Schulung dazu vorbereitet, wie sie ihren privaten Mailverkehr mittels mehrstufiger Nutzer-Identifizierung (MFA) sichern können und warum auch ihre nächsten Angehörigen dieses Instrument nutzen sollten.

„Ein Großteil unserer Arbeit besteht deswegen aus eindringlicher Bewusstmachung, wie wichtig Cyberhygiene ist“.

Jeder Mensch hat sein Privatleben und oftmals ist es nicht möglich, sich hier einzumischen oder jemanden zu zwingen bestimmte Verhaltensweisen zu beachten.

Meiner Meinung nach, war einer der Gründe, weshalb unsere Gegner in private E-Mail-Postfächer eingedrungen sind, dass sie es nicht schaffen unsere militärischen IT-Systeme zu knacken. In vielen Fällen war hierzu bei den privaten E-Mail-Adressen lediglich ein Login und ein

Passwort erforderlich, was für jeden, der auch nur ein bisschen Ahnung von Social Engineering hat, ein Kinderspiel ist. Diese Methoden sind seit den Zeiten von Kevin Mitnick bekannt, der in den 1980er Jahren per Telefon Passwörter zu geheimen Systemen des US-Außenministeriums ausspionierte.

Kann man erwarten, dass die Hintermänner dieser Hackerangriffe auf E-Mail-Lacks bestraft werden?

Solche gefährlichen Aktivitäten im Cyberspace werden uns so lange begleiten, bis die Internetnutzer sich der damit verbundenen Risiken bewusst werden. Leider ist dies ein globales Problem. Nicht nur in Polen sind E-Mails von wichtigen Beamten durchgesickert. In den Vereinigten Staaten sind solche Vorfälle fast an der Tagesordnung, obwohl das Land enorme Ressourcen für die Cybersicherheit bereitstellt.

Denn wenn man die Internetnutzer wirksam vor solchen Lacks schützen wollte, müsste man ihre privaten Postfächer überwachen, und wir möchten nicht in einem Land leben, in dem es eine Institution mit solchen Befugnissen gibt. Deshalb können wir nur Hinweise geben und warnen.

Bald, nach vier Jahren der Vorbereitung, wird es endlich eine neue Komponente der Streitkräfte geben: Cyber-Verteidigungskräfte (WOC). Wann werden wir bereit sein, einen Angriff auf den Feind zu starten?

Unsere Teams bauen solche Kompetenzen auf oder haben sie bereits aufgebaut. Zurzeit nutzen wir unsere offensiven Ressourcen, um die Sicherheit unserer Systeme zu überprüfen. Denn es müssen rechtliche Lösungen gefunden werden, um beispielsweise zu definieren, wie militärische Teams in Friedenszeiten für Cyberoperationen eingesetzt werden können.

Dieses Thema wird im Rahmen der Arbeiten am Gesetzentwurf zur Landesverteidigung erörtert, in dem die Definition der Cyber-Verteidigungskräfte enthalten ist. Diese Frage erfordert eine Entscheidung auf strategischer Ebene.

„Wir sollten von den Erfahrungen unserer Partner profitieren“.

Wir sollten von den Erfahrungen unserer Partner profitieren. In den Vereinigten Staaten verfügt der Befehlshaber einer Cyber-Armee über eine sogenannte Executive Order – eine Ermächtigung des Präsidenten, im Falle eines Cyberangriffs auf die USA eine angemessene Vergeltungs-maßnahme durchzuführen. Er kann also sofort reagieren. Wenn er auf die Genehmigung des Präsidenten warten müsste, könnte das Stunden oder Tage dauern, und bei einem Cyberangriff ist das eine sehr lange Zeit.

Warschau im Juni 2019. US-Brigadegeneralin Maria Biank und Brigadegeneral Karol Molenda nach der Unterzeichnung eines Ko-operationsabkommens zwischen dem United States Cyber Command und dem polnischen Nationalen Zentrums für Cybersicherheit.

Wie viele Soldaten werden in den Cyber-Verteidigungskräften (WOC) die-nen?

Die genaue Zahl wird nicht mitgeteilt. Derzeit umfasst unsere Struktur – NCBC und direkt unterstellte Einheiten – mehr als 6.000 Vollzeitsoldaten und zivile Mitarbeiter. Diese Personen sind nicht nur für den Cyberspace, sondern auch für IT oder Kryptologie zuständig. Das mag nicht viel erscheinen, aber im Vergleich dazu hat das US-Cyber-Militär 7.000 bis 8.000 Soldaten.

NCBC-Erkennungsmerkmal. Aufnäher am rechten Uniformärmel.

Wichtig ist nicht die Quantität, sondern die Qualität. Die größte Herausforderung besteht heute darin, kompetente Teams aus hochrangigen Spezialisten zusammenzustellen. Das ist sehr schwierig. Schätzungen zufolge fehlen allein in Europa drei Millionen Cyber-Sicherheitsexperten.

Wie also kann man Fachleute mit einzigartigen Fähigkeiten davon überzeugen, dass es sich lohnt, den WOC beizutreten?

Wir zeigen die Perspektiven auf, die sich hochkarätigen Experten, die bei uns dienen, eröffnen. Natürlich kann man auf dem privaten Markt mehr Geld verdienen, aber dann ist man nur ein Rädchen, das Gewinne für die Konzerne erwirtschaftet.

Internetanzeige. „Das Militär baut eine Cyber-Armee auf und sucht Informatiker.“

Andererseits können sie bei uns ihrem Heimatland dienen und unmittelbar mit dem Feind in Berührung kommen, z. B. mit den sich weiterentwickelnden APT-Gruppen, die komplexe, zielgerichtete und sehr effektive Angriffe auf kritische IT-Infrastrukturen und vertrauliche Armeedaten starten. Sich mit ihnen zu messen ist eine der anspruchsvollsten Herausforderungen für einen IT-Experten.

Und was ist mit dem Geld? Wie viel kann ein solcher Spitzenexperte heutzutage in der Armee verdienen?

Wie ich bereits sagte, werden auf dem privaten Markt heute höhere Gehälter gezahlt als bei uns am NCBC. Das könnte sich jedoch bald ändern. Es ist ein Gesetz in Kraft getreten, das es ermöglicht, Cyber-Sicherheitsexperten mit einzigartigen Kompetenzen angemessen zu entlohnen.

Derzeit wird in der Kanzlei des Premierministers an einer Verordnung gearbeitet, in der alle damit zusammenhängenden Einzelheiten, einschließlich der möglichen Gehaltsspannen, festgelegt werden. Ich möchte zum jetzigen Zeitpunkt keine konkreten Beträge nennen, aber ich bin optimistisch.

Zu diesem Thema auch lesenswert:

Wohin marschiert die polnische Armee

RdP

Das Gespräch erschien im Wochenmagazin „Gazeta Polska“ („Polnische Zeitung“) vom 6. Januar 2022.