They leak twice: Tusk government unaware for two years of data breach affecting 19 million Poles

epa11421851 Polish Minister of Digital Affairs Krzysztof Gawkowski has attended scores of cybersecurity forums. The reported leak of 19 milli0on Polesperosnal and medical records will no doubt be debated at future ones. EPA/LUKASZ GAGULSKI

He said that "we are dealing with an extraordinary and very large incident in terms of the security of Poland's information sphere".
Polish deputy digital affairs minister Michał Gramatyka has said that he had no knowledge of a leak involving the medical data of nearly 19 million Poles that occurred as far back as two and a half years ago.

On August 12, digital affairs minister Krzysztof Gawkowski, who is also deputy prime minister, admitted that data concerning 19 million Poles held by MyDr had been leaked but that the leak had occurred in recent days.

He said that “we are dealing with an extraordinary and very large incident in terms of the security of Poland’s information sphere”.

The offence under investigation carries a possible prison sentence of up to two years under article 267 of the Polish penal code.

The matter was first reported on August 10 by *Zaufana Trzecia Strona*, an IT security news service, which said that it had been contacted on August 8 by the alleged perpetrators, who claimed to have accessed the data of around 18.8 million people. They put the figure at 18,814,422 unique identification numbers.

The hackers, who have not been identified, had also sent a screenshot from the compromised database showing the personal data of “one of the most important politicians in Poland” to the news service.

Warsaw district prosecutors are investigating unauthorised access to MyDr’s systems obtained no later than August 6. The breach targeted records of MyDr, one of the country’s largest electronic medical-record providers, including prescription, medication and other sensitive patient data. Gawkowski said the stolen database exceeded 2 terabytes.
Around 12,000 medical facilities use MyDr’s services with the company processing 3 million medical consultations and 2.7 million prescriptions a month.

The Warsaw District Prosecutor's Office said the compromised information included names, PESEL identification numbers, phone numbers and email addresses, as well as sensitive health information such as notes from medical appointments and prescription details.

But news website *Niezależna* on August 17 reported that a similar incident had already taken place two and a half years ago involving almost exactly the same number of data records.
Between March 18 and 27, 2024, hackers obtained the data of 18,814,054 Poles comprising not only their names, but also their identity (PESEL) numbers and information on whether they had valid health insurance coverage.

The Regional Prosecutor's Office in Poznań, western Poland, opened an investigation into the case but the Ministry of Digital Affairs was not informed about either the leak or the investigation. The data protection authority, UODO, was also not notified.
Poznań prosecutors confirmed the account on August 18, saying the inquiry had been opened on April 8, 2024, on notification from the president of the National Health Fund (NFZ), and that two people have been charged.

Their statement described a different method from the current case. An intruder broke into the network of a medical centre, then implanted a script in MyDr that sent some 18 million automated queries to the NFZ's patient-entitlement verification system, eWUŚ. On that account, prosecutors said the perpetrators obtained the data of more than 13 million people, not 18.8 million.

Zaufana Trzecia Strona has said the two episodes are separate incidents despite the near-identical victim counts.

Shortly after the *Niezależna* article was published Gramatyka confirmed that he had not previously been aware of the incident.

"I only learned about this whole matter just now, at the same time as you did," he told journalists, adding that he did not believe "such a large batch of data was leaked in March 2024 and that these were two separate incidents".

But according to a document from the prosecutor's office seen by *Niezależna* the action occurred in 2024 and concerned "the personal data of 18,814,054 individuals was unlawfully obtained, including their names and PESEL numbers, thereby causing harm to the National Health Fund (Poland's national health service contracting agency)".

On August 13 Polish Prime Minister Donald Tusk said that the cyberattack on the data of nearly 19 million people revealed by Gawkowski appeared to have been a criminal attempt to extort a ransom from MyDr itself.

"The motivation appears to be purely criminal. There are many indications that this was an attempt to extort a ransom," he said, adding that the attack involved "very sophisticated" methods. He also said no private-sector system anywhere could be guaranteed against attack.

Gawkowski has said that the stolen records have not appeared in the public domain nor been offered for sale and that thus far there was no evidence of foreign involvement.
The digital affairs minister had to concede though that there could be no guarantee that the records would not eventually be leaked as the government would not negotiate with those responsible for the incident.

"The ministry and state services do not negotiate with hackers. We hunt criminals down; we do not strike deals with them," he said.

Gawkowski urged all members of the public to use the option of making their PESEL numbers confidential, which blocks them from potential use by fraudsters. The Polish Bank Association issued the same advice.

The authorities have promised to enable citizens to check through the government-run Bezpieczne Dane ("Safe Data") portal whether their personal information was among the compromised records. As of August 16, the MyDr set had still not been loaded onto it.
Minister Gawkowski has also said that Poland's Cyberspace Defence Forces, a part of Poland's military specialising in cyber security, would receive additional funding.

The minister failed to explain how a hack of the data of nearly 19 million people from 2024 could be repeated at a time when the country fears Russian hackers attempting to extract information with which they can extort ransoms from institutions and individuals.

The leaked data included soldiers, intelligence officers, politicians, government officials and journalists, serving as a highly valuable source of information.

Experts warn that Poland remains a prime target of coordinated attacks by hostile states and cybercriminals, while the national response system is still fragmented, reactive and too slow. A study by the Basque industrial cybersecurity centre ZIUR placed Poland first in Europe for politically motivated attacks in the second quarter of 2025, ahead of Ukraine and Israel.
Cyberattacks in Poland have reached a record scale. In 2024 alone, CERT Polska recorded over 600,000 reports of cyber incidents, an increase of 62 per cent compared to the previous year. National response teams confirmed 111,660 of them as actual security incidents.

The most frequently reported type of attack was phishing, but new forms of social engineering fraud have also gained popularity, such as fake summons from the police, fines with QR codes, or messages "from a child" from a new number.

At the same time, actual readiness to counter these threats, both in the public and private sectors, remains weak. In many offices staff still use public email accounts and sign IT contracts without security clauses.

According to the lobby group Digital Poland Association, eliminating regulatory chaos, accelerating the legislative process in Poland, implementing Zero Trust security architecture, mandatory cybersecurity training for public and private sector employees, and requiring digital solutions to be designed according to the "Secure by Design" principle are the key needs of the sector.

Though what concerned the authorities the most were 450 incidents that were politically motivated and were diverse, using denial of service, ransomware, data theft and leaks and malware attacks.

These attacks predominantly targeted critical sectors, including government institutions, the energy sector, non-governmental organisations and media outlets. The surge in cyber hostilities, the authorities believe, can be attributed to the activation of pro-Russian groups, who have intensified their operations since Russia's invasion of Ukraine.

But despite the concern, thus far the government has warned the public while remaining unaware of a data leak years after it happened, amid confusion over whether the same data may have been leaked twice.

The incident with the 19 million leak may not be as serious as the Russian drone incursion of September 2025 or the July 2026 incident in which a Russian Kh-101 cruise missile crashed into a field at Tarnawa-Kolonia, Lublin province, eastern Poland, after travelling for six minutes inside Polish territory without any attempt to shoot it down, but it has revealed similar concerns about the government's response.

The stray Russian missile revealed that the alert system was largely ineffective, with sirens sounding but no timely warning message reaching residents. Days later, on July 31, the Government Security Centre sent a nationwide alert containing a link to an online safety handbook, having warned in 2024 that genuine alerts

never carry links. Government websites slowed under the traffic, though Gawkowski denied there had been any outage.

The Polish public must now hope that lessons will be learned and that there will be no third time for those wanting to cause the country some harm.

Author:

Krzysztof Mularczyk
European Conservative, fotopolis.pl, Warsaw Correspondent for Brussels Signal

Source: Brussels Signal

Photos: EUR. EPA/LUKASZ GAGULSKI