CYBERMINUTE

Alberta Cybersecurity Insights

TLP:CLEAR

Data Breach Fallout: Lessons from National Public Data and Edmonton Incidents

In April 2024, a cybercriminal threat actor known as USDoD claimed the compromise of National Public Data (NPD) and attempted to allegedly sell 200 GB of stolen data. This data consisted of approximately 2.7 billion records of personal information on residents in the US, Canada, and the UK. After failing to secure a buyer, the data was leaked in stages, with the most comprehensive version released in August on a cybercriminal forum.

The leaked records include sensitive information such as Social Security Numbers (SSNs), names, email addresses, home addresses, dates of birth, and more. Analysis of the data found inconsistencies suggesting the leaked data was not entirely accurate. However, the breach still impacted many people's data and has led to many class-action lawsuits citing inadequate security measures and delayed response in informing affected individuals.

Another breach also occurred in August affecting multiple Edmonton based public sector organizations. Unlike the NPD compromise, this breach did not involve a cyber-attack but was the result of unauthorized access granted by a City of Edmonton contractor to a third-party. Names, dates of birth, and pension details belonging to public sector employees were

inadvertently exposed. The exposure was quickly remediated, and the contractor's account was immediately revoked, but this error demonstrates how internal mishandling of data can lead to significant privacy breaches.

Data exposed via breaches can potentially be leveraged by threat actors as part of further cyber-attacks such as identity theft, fraud, or phishing. As a result, individuals impacted by such breaches are urged to take several protective steps:

- Monitor credit reports for any anomalous activity.
- Freeze accounts to prevent fraudulent attacks.
- Replace passwords of any affected accounts.
- Enable multi-factor authentication (MFA).
- Remain cautious of phishing attempts that might exploit the exposed data.

The NPD breach has prompted calls for stronger oversight of companies handling large volumes of personal information, and for greater accountability in the protection of sensitive data. Organizations handling data can prevent inadvertent data leakage by implementing the following recommendations:

- Enforce access controls to ensure sensitive data is only accessible to authorized personnel.
- Monitor and audit access logs to detect anomalous activity.
- Implement Data Loss Prevention (DLP) policies regarding the sharing and storage of data.

For further Cybersecurity useful tools, such as best practices and playbooks, visit the CyberAlberta website.

Click Here to Read More!

Cyber Attacks on the Rise: Canadian Farmers Targeted by Ransomware

The agriculture sector, a critical component of the nation's economy and food security, has become a prime target for cybercriminals. Recent reports indicate a surge in ransomware attacks on Canadian food and agriculture industries, causing substantial financial losses and operational disruptions. Alberta—with its vast agricultural landscape—is not immune to these threats. The province's reliance on technology for farming operations makes it vulnerable to cyber-attacks that could compromise food production and distribution systems.

The implications of such attacks are far-reaching, as a ransomware incident can lead to the loss of critical data, financial extortion, and in severe cases, a complete halt in operations. This could mean empty supermarket shelves, increased food prices, and a blow to local economies. The interconnectedness of modern supply chains further exacerbates the problem, as a single breach can ripple through the network, affecting suppliers and consumers alike.

Recent ransomware attacks have brought significant challenges to Canadian farms.

Microsoft Announces Mandatory MFA Rollout for Azure Sign-in

On August 15, 2024, Microsoft announced that it will require mandatory MFA for all Azure sign-ins. This move aims to enhance the security of identities and sensitive data by minimizing the risk of unauthorized access. Microsoft's research shows that MFA is 99.2% effective as a deterrent, making it an extremely potent control.

What does this change mean for you? Beginning in October, Microsoft will start the first phase of their rollout. During this period, mandatory MFA will be gradually enforced for your tenants when using Azure portal, Microsoft Entra admin center, or Intune admin center. In early 2025, Microsoft will enter the second phase, progressively enforcing MFA for Azure Command Line Interface, Azure PowerShell, the Azure mobile app, and Infrastructure as Code tools.

To help customers prepare for this transition, Microsoft has issued a 60-day advance notice to all Entra global admins via Azure Service Health Notifications and email. This email contains the start of enforcement for your tenant, and the actions you need to take.

There has been a string of attacks linked to Russian groups, which have targeted Canada's food and agriculture industry, causing disruptions that had a knock-on effect on supply chains and operations. An example of this could be seen in a 2022 attack on Sobeys which resulted in over $30 million in losses due to spoilage, repairs, and lost sales.

Grocery stores have not been the only ones impacted by these cyber-attacks. The agricultural association Ontario Pork experienced two separate cybersecurity incidents last year, both reported by the dark-web monitoring site RansomLook. This year, both Lactanet—a dairy data firm, and Agropur—a dairy co-op—had their data compromised in similar ransomware attacks. Most recently, Federated Co-operatives—a major food supplier in Western Canada—suffered a ransomware attack leading to weeks of empty shelves at numerous stores across the region.

In response to these threats, it is imperative for food producers and distributors to implement robust cybersecurity measures. Consumers and businesses alike must understand the potential risks and support initiatives aimed at strengthening the digital resilience of the food industry. As ransomware attacks become more sophisticated, a collective effort is required

By enforcing MFA within the Azure tenant, Microsoft can greatly reduce the risk of unauthorized access to sensitive data. However, such changes can pose a significant risk, especially for organizations with large, complex environments where such transitions may present technical challenges. Consider how prolonged interruptions to authorized access could impact your organization. We recommend that users start preparing for and managing these changes now to ensure a smooth transition to mandatory MFA.

Click Here to Read More!

to safeguard Alberta's food supply from these cyber threats.

Click Here to Read More!