{e}mazzanti® technologies
TECHNOLOGY STRATEGIES FOR BUSINESS GROWTH.

Microsoft Ukraine and Cybersecurity - How Microsoft is Helping and What That Means to You

As a Microsoft Partner and representative of its products, eMazzanti Technologies is naturally concerned about digital technology and the war in Ukraine. Indeed, Microsoft, Ukraine, and cybersecurity have become areas of increasing interest for eMazzanti and its customers. Hence, we share this update of Microsoft's efforts to help.

In a February 28, 2022, post, Brad Smith, Microsoft President & Vice Chair related,
"This has become both a kinetic and digital war, with horrifying images from across Ukraine as well as less visible cyberattacks and disinformation campaigns."

Smith goes on to explain how Microsoft is working in four areas to help:

- Protecting Ukraine from cyberattacks
- Protection from state-sponsored disinformation campaigns
- Support for humanitarian assistance
- And the protection of its employees

Microsoft's efforts have involved constant and close coordination with the Ukrainian government, the European Union, European nations, the U.S. government, NATO, and the United Nations.

1. Protection from Cyberattacks

One of Microsoft's principal and global responsibilities as a company is to help defend governments and countries from cyberattacks.

Several hours before the launch of missiles or movement of tanks on February 24, Microsoft's Threat Intelligence Center (MSTIC) detected a new round of cyberattacks. These offensive and destructive attacks targeted Ukraine's digital infrastructure.

The center immediately advised the Ukrainian government about the situation. Intelligence indicated the use of a new malware package (FoxBlade). The center also provided technical advice on steps to prevent the malware's success.

As part of an ongoing effort, they also provided threat intelligence and defensive suggestions to Ukrainian officials. They advised officials on a range of targets, including Ukrainian military institutions, manufacturers, and other government agencies.

The company noted a special concern about recent cyberattacks on Ukrainian civilian digital targets. Those targets included the financial and agriculture sectors, emergency response services, humanitarian aid efforts, and energy enterprises.

They also advised about recent cyber efforts to steal a wide range of data, including health, insurance, and transportation-related personally identifiable information (PII). In addition, the company constantly updates Microsoft services, including Defender, to help protect against the spread of malware to other customers and countries.

2. Protection from State-Sponsored Disinformation

Microsoft is also focused as a company on protecting against state-sponsored disinformation campaigns, which have been common in times of war.

In accordance with the EU's recent decision, the Microsoft Start platform (including MSN.com) will not display any state-sponsored RT and Sputnik content. And the company is banning all advertisements from RT and Sputnik across its ad network.

3. Support for Humanitarian Aid

Microsoft's initial and immediate focus has been on support for humanitarian organizations such as the ICRC. That group performs critical work to help support refugees fleeing into neighboring countries. Leadership also activated the Microsoft Disaster Response Team to provide technology support. They are in frequent touch with additional first responders to provide help.

Microsoft is also leveraging other parts of its business to help the public find and support humanitarian organizations. They encourage and are seeing an outpouring of generosity from employees in the United States, Europe, and around the world through Microsoft's employee giving program.

4. Protection of Employees

Microsoft has employees located around the world, including in Ukraine, Russia, and across eastern Europe. The company also has many employees of both Ukrainian and Russian origin working in other locations.

Like other multinational companies, Microsoft is devoted to the protection of its employees. This includes ongoing and extraordinary efforts by its teams to help employees and families, including those who have fled for their lives or safety.

Disrupting Cyberattacks Targeting Ukraine

In an April 7, 2022, post, Microsoft shared more about cyberattacks they've seen from a Russian nation-state actor targeting Ukraine. They recently observed and disrupted attacks from Strontium, a Russian GRU-connected actor they have tracked for years.

On April 6th, they obtained a court order authorizing Microsoft to take control of seven internet domains Strontium was using to conduct these attacks. They quickly re-directed these domains to a sinkhole controlled by Microsoft, making them useless and enabling victim notifications.

Strontium was using this infrastructure to establish long-term access to the systems of Ukrainian institutions including media organizations. It was also targeting government institutions and think tanks in the United States and the European Union involved in foreign policy.

> *These attacks were intended to provide tactical support for the physical invasion and steal sensitive information.*

Prior to this week, Microsoft had acted through this process 15 times to seize control of more than 100 Strontium controlled domains.

Before the Russian invasion, Microsoft teams began working around the clock to help organizations in Ukraine, including government agencies, defend against the relentless cyberwarfare that has escalated since the invasion began.

Since then, they have observed nearly all of Russia's nation-state actors engaged in the ongoing full-scale offensive against Ukraine's government and critical infrastructure. They continue to work closely with government and organizations of all kinds in Ukraine to help them defend against this onslaught.

Microsoft Ukraine and Cybersecurity Shared

Long before the invasion of Ukraine, Microsoft had observed destructive malware in systems belonging to several Ukrainian government agencies and connected organizations. They shared this information to help others in the cybersecurity community look out for and defend against these attacks.

Microsoft said they built and deployed protections for this malware into Microsoft 365 Defender Endpoint Detection (EDR) and Anti-virus (AV) protections wherever these products are deployed, both on-premises and in the cloud. They see no indication so far that these attacks utilize any vulnerability in Microsoft products and services.

eMazzanti Technologies takes Microsoft, Ukraine, and cybersecurity very seriously. We do all in our power to protect our customers' vital business assets from ransomware attack and other threats. Our cybersecurity experts develop multi-layered cybersecurity defense strategies for businesses of all sizes around the world.