REN-ISAC

Tension in Ukraine: Mitigating Effects on Higher Education

TLP: WHITE

As tensions continue to escalate between Russia and the Ukraine, we as information security professionals need to take immediate steps to review, test, and upgrade our incident response practices in preparation for a possible nation-state sponsored attack. Nation-state actors have a history of infiltrating supply chains, critical systems, and data stores to attack US Critical Infrastructure, and the rise in political tensions will probably only cause them to strike harder.

Protecting Organizational Systems

As small communities that hold vast amounts of personal and research data, higher education and research is a prime target for nation-state attacks. To prepare for nation-state attacks, organizations need to review incident response strategies for attacks on

- Their own organizational networks.
- Student and research networks they secure.
- Networks of key partners or suppliers that impact daily institutional functions.
- Networks of organizations and companies in other critical infrastructure sectors that have cascading impacts on research and education institutions.

Mitigating this issue:

Now is the time to review your current data management and security procedures and policies to make sure they are up-to-date and well-practiced. We suggest higher ed security leaders

- Meet with their incident response teams.
- Review their business continuity plans.
- Discuss threat with organizational executives.
- Organize a table-top exercises with relevant stakeholders.

Protecting International Students, Faculty, and Their Data

Higher ed institutions house international students, faculty, and staff from the affected areas. We need to be able to protect them and protect their data. International students, faculty, and staff might be unable to return to their place of origin, lose their immigration status due to change of leadership in place of origin, or lose access or control over data housed in impacted areas.

Mitigating this issue:

Your organization and IT professionals can help individuals impacted by this situation, as well as protect data and research of those traveling in or near impacted areas, by

- Reaching out to your organization’s international student, faculty, staff support offices.
- Reviewing your organization’s policies for international travel.
- Reviewing your information security standards for international travel.

REN-ISAC

For More Information

International Travel Resources

- Ukraine Travel Advisory, U.S. Department of State—Bureau of Consular Affairs
- Information for U.S. Citizens in Ukraine, U.S. Department of State—Bureau of Consular Affairs
- Foreign travel advice—Ukraine, Gov.UK
- Effective Practices: Cybersecurity and International Travel Series" (TLP:WHITE) with guidance checklists for both the international traveler and the IT support professional, REN-ISAC

Cybersecurity & Infrastructure Agency (CISA) Alerts

- Sheilds Up Advisory
- Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure
- Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology
- Russia Cyber Threat Overview and Advisories

National Cyber Security Centre (NCSC) Alerts

- UK Organisations Encouraged to Take Action in Response to Current Situation in and Around Ukraine (NCSC)

The White House/U.S. Presidential Briefings

- FACT SHEET: Act Now to Protect Against Potential Cyberattacks

Incident Response Resources

- Incident Response Playbooks, National Student Clearing House

Business Continuity Resources

- Continuity of Operations (COOP), Federal Emergency Management Agency (FEMA)
- Business Continuity and Disaster Recovery, Educause

Tabletop Resources

- Blended Threat Workshop Final Report with best practices for ransomware incidents, REN-ISAC
- Campus Resilience Program, U.S. Department of Homeland Security

General Resources

- Executive Overview of Russian Aggression Against Ukraine, Insikt Group
- Russia's Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine (Updated Feb. 16), Palo Alto
- The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict, Harvard Business Review
- Nation State Threat Actors: From a Security Awareness Perspective, SANS