techr2

Threat Announcement - 2022 Industry Weaknesses

2022 Across the Industry Findings – Security

1. Organizations allow processing of physical data bearing devices outside of the secure datacenter or offsite and out of their control which is in direct violation of federal, state and industry regulations.
2. Co-location data centers may allow computer technicians to exit their datacenters without any physical security check which could allow data bear devices (DBDs) to be taken out.
3. Enterprise offices have only a fraction of the security that a datacenter has and are vulnerable to compromise.
4. Third party sub-contractors do not have the proper information security credentials required by law or industry standards. Sub-contractors utilize weak industry certifications versus undergoing Cyber Security Framework (CSF) certification.
5. Third party providers sub-contract the work to another company. The next level providers do not have data security credentials and are not approved by the customer.
6. Company datacenters on the whole do not properly contain the DBDs. Most often they are placed in boxes, in desks or on shelves.
7. No inventory is completed for IT assets or DBDs, so organizations are unable to determine when a loss occurs or what is missing.
8. Security measures for mobile devices may not be in place to protect information from loss.
9. Access control and management of user rights is not being implemented and reviewed at intervals.
10. Two factor authentication is not being used as an extra layer of security for accessing critical data.

2022 Across the Industry Findings – Management

1. No written plan or budget that accounts for storage servers or devices from cradle to grave is in place.
2. Organizations lack a budget to perform proper data security. In many cases, non-skilled personnel and unverified software are being used.
3. Senior data engineers and security managers are not present to verify critical data interaction.
4. Software and hardware are used that do not conform to Cyber Security Framework (CSF) guidelines. Software used does not remove the data, and data files can be found with recovery software.
5. Existing policies and procedures are out of date. Compliance and risk managers are ill advised. Independent review for information security compliance with standards is not completed.
6. Incident Response responsibilities and procedures are not established and tested regularly.
7. Information Security Continuity is not addressed. Policies and procedures are not written, verified, reviewed, and evaluated.
8. Datacenter or enterprise facility is missing a Risk Assessment that is approved by the organization's compliance officer for the location.

2022 Across the Industry Findings – Skill

1. OEM manufacturers contracts are not compliant with current NIST and GDPR regulations. Data is sent on equipment to non-compliant OEM manufacturers as part of maintenance contracts. OEMs are using non-compliant sub-contractors.
2. There is no tracking of data to within regulation guidelines.
3. Data Bearing Devices (DBDs) are not tracked when removed from the host system. Only a few datacenters nationwide have an accurate and up-to-date inventory of critical data bearing equipment and devices.
4. Organizations have existing internal procedures and policies that allow them to bypass US NIST and other industry standards. Critical data procedures are incomplete and are not verified.
5. Equipment used for media sanitization does not meet NSA guidelines.

2022 Across the Industry Findings – Training

1. Single operators are interacting with data when alone. The organization does not use a verifier as required by current regulations.
2. Organizations do not use a verification method to test data bearing devices are sanitized before the equipment leaves the organization's control.
3. There is a lack of training for professionals who interact with data. No certification documents or out of date certifications are on file.
4. Inadequate data migration and data eradication techniques are being used. Many organizations use incomplete encryption or factory reset procedures, and the data can be recovered on the DBDs by a professional.
5. Machines used in the datacenter or enterprise do not contain UL or CSA certification or validation documentation.
6. Individuals with security credentials compromise their certified security training to comply with the organization's non-compliant policies.
7. Information Security Awareness education and training for all employees is not provided or documented.
8. Training for reporting and responding to Security Events for all employees is not provided or documented.
9. Insider Threat training is not provided or documented.

techr2 Media Security Solutions. **techr2.com**
12477 Broad St. SW, Pataskala, Ohio 43062 | 614.322.2222 | clientrelations@techr2.com

TEAR-A-BYTE PATENTED PROCESS Achieve GDPR COMPLIANCE