How Gov Gets Hacked

Malware

Malicious computer code used to corrupt, destroy, or steal digital information. Malware includes viruses and worms, in addition to spyware that monitors user activity and ransomware that holds data hostage.

In 2012, the South Carolina Department of Revenue experienced one of the largest malware attacks in history when an employee unwittingly clicked a malicious link in a phishing email.

In 2013, hackers exploited a known flaw in an enterprise web platform to access the Department of Energy’s DOEInfo employee database.

Malicious Insider Threats

Employee use of government personnel, facilities, information, equipment, networks, or systems to inflict harm on the organization. Insider threats can take many forms, from releasing confidential information to deploying advanced malware from within a network firewall.

In 2010, Chelsea Manning, born Bradley Manning, worked as an Army Intelligence Analyst where she had access to the Defense Department’s Secret Internet Protocol Router Network (SIPRNet). Manning accessed material from the network and passed it to Wikileaks.

Zero Day Attack

An exploitation of unknown or undisclosed computer application vulnerabilities to access, disrupt, or damage networks.

In 2013, hackers exploited a known flaw in an enterprise web application to access the Department of Energy’s DOEInfo employee database.

Zero Day Attack

A level of service tactic for prevention of denial of service. An interruption of network service, executed by sending such high volumes of traffic or data to a single network that it becomes overloaded and inoperable.

In February 2015, hackers sent a flood of emails to multiple municipal departments for the city of New York, effectively shutting down communications between city offices as well as the local FBI office and the NYPD.

Distributed Denial of Service

An interruption of network service, executed by sending such high volumes of traffic or data to a single network that it becomes overloaded and inoperable.

In February 2015, hackers sent a flood of emails to multiple municipal departments for the city of New York, effectively shutting down communications between city offices as well as the local FBI office and the NYPD.

Prevention Tactics

1. Education: Educate employees on cybersecurity best practices.
2. Environment: Secure data across all devices and environments.
3. Segmentation: Segment your network and data.
5. Compliance: Comply with relevant laws and regulations.
6. Mitigation: Mitigate potential threats through proactive IT risk assessment.
8. Testing: Conduct regular IT security audits and penetration testing.
11. Mitigation: Mitigate potential threats through proactive IT risk assessment.
13. Testing: Conduct regular IT security audits and penetration testing.

Prevention Tactics

1. Education: Educate employees on cybersecurity best practices.
2. Environment: Secure data across all devices and environments.
3. Segmentation: Segment your network and data.
5. Compliance: Comply with relevant laws and regulations.
6. Mitigation: Mitigate potential threats through proactive IT risk assessment.
8. Testing: Conduct regular IT security audits and penetration testing.
11. Mitigation: Mitigate potential threats through proactive IT risk assessment.
13. Testing: Conduct regular IT security audits and penetration testing.

Prevention Tactics

1. Education: Educate employees on cybersecurity best practices.
2. Environment: Secure data across all devices and environments.
3. Segmentation: Segment your network and data.
5. Compliance: Comply with relevant laws and regulations.
6. Mitigation: Mitigate potential threats through proactive IT risk assessment.
8. Testing: Conduct regular IT security audits and penetration testing.
11. Mitigation: Mitigate potential threats through proactive IT risk assessment.
13. Testing: Conduct regular IT security audits and penetration testing.

Prevention Tactics

1. Education: Educate employees on cybersecurity best practices.
2. Environment: Secure data across all devices and environments.
3. Segmentation: Segment your network and data.
5. Compliance: Comply with relevant laws and regulations.
6. Mitigation: Mitigate potential threats through proactive IT risk assessment.
8. Testing: Conduct regular IT security audits and penetration testing.
11. Mitigation: Mitigate potential threats through proactive IT risk assessment.
13. Testing: Conduct regular IT security audits and penetration testing.

Prevention Tactics

1. Education: Educate employees on cybersecurity best practices.
2. Environment: Secure data across all devices and environments.
3. Segmentation: Segment your network and data.
5. Compliance: Comply with relevant laws and regulations.
6. Mitigation: Mitigate potential threats through proactive IT risk assessment.
8. Testing: Conduct regular IT security audits and penetration testing.
11. Mitigation: Mitigate potential threats through proactive IT risk assessment.
13. Testing: Conduct regular IT security audits and penetration testing.

Prevention Tactics

1. Education: Educate employees on cybersecurity best practices.
2. Environment: Secure data across all devices and environments.
3. Segmentation: Segment your network and data.
5. Compliance: Comply with relevant laws and regulations.
6. Mitigation: Mitigate potential threats through proactive IT risk assessment.
8. Testing: Conduct regular IT security audits and penetration testing.
11. Mitigation: Mitigate potential threats through proactive IT risk assessment.
13. Testing: Conduct regular IT security audits and penetration testing.

Prevention Tactics

1. Education: Educate employees on cybersecurity best practices.
2. Environment: Secure data across all devices and environments.
3. Segmentation: Segment your network and data.
5. Compliance: Comply with relevant laws and regulations.
6. Mitigation: Mitigate potential threats through proactive IT risk assessment.
8. Testing: Conduct regular IT security audits and penetration testing.
11. Mitigation: Mitigate potential threats through proactive IT risk assessment.
13. Testing: Conduct regular IT security audits and penetration testing.

Prevention Tactics

1. Education: Educate employees on cybersecurity best practices.
2. Environment: Secure data across all devices and environments.
3. Segmentation: Segment your network and data.
5. Compliance: Comply with relevant laws and regulations.
6. Mitigation: Mitigate potential threats through proactive IT risk assessment.
8. Testing: Conduct regular IT security audits and penetration testing.
11. Mitigation: Mitigate potential threats through proactive IT risk assessment.
13. Testing: Conduct regular IT security audits and penetration testing.

Prevention Tactics

1. Education: Educate employees on cybersecurity best practices.
2. Environment: Secure data across all devices and environments.
3. Segmentation: Segment your network and data.
5. Compliance: Comply with relevant laws and regulations.
6. Mitigation: Mitigate potential threats through proactive IT risk assessment.
8. Testing: Conduct regular IT security audits and penetration testing.
11. Mitigation: Mitigate potential threats through proactive IT risk assessment.
13. Testing: Conduct regular IT security audits and penetration testing.