MITIGATE CYBERSECURITY RISKS WITH PRE-TESTED SECURITY UPDATES

SECURITY PATCH INSTALLATION FOR MISSION-CRITICAL COMMUNICATION SYSTEMS

COMMUNICATION SYSTEMS FACE INCREASED CYBERSECURITY RISKS

The transformation of mission-critical communications systems to IP based environments and ability to connect to like systems have allowed for the introduction of new capabilities for improving operational efficiencies and intelligence. Like any other IP-based system, today's critical communication networks are not immune from cyber attacks. You can mitigate this risk by addressing known vulnerabilities as soon as the required security updates are available.

MAINTAIN COMPLIANCE

Pre-testing and validation procedures enable adherence to various government mandates, specific market regulations and industry best practices set for increased system cybersecurity measures including:

- Federal Information Security Management Act (FISMA)
- Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)
- Department of Homeland Security Policy 4300A
- National Institute of Standards Technology: NIST 800-53
- North American Electric Reliability Corporation (NERC)
- ISO 27001
- Payment Card Industry (PCI) Security Standards
- Other privacy directives

PRE-TEST SOFTWARE UPDATES TO PROTECT CONTINUITY OF SYSTEM OPERATIONS

Robust system patching capability is an integral part of the overall organization's cybersecurity program. Industry best practices suggest that software patches are applied as soon as possible after release from the vendor. However, testing software updates before deploying on a mission critical system is absolutely essential.

Motorola's Security Update Service pre-tests the latest anti-malware definitions and all applicable software patches in dedicated test labs. Only the applicable patches needed for the system are identified and selected for testing. This validates that no unnecessary software is introduced via the patching process. Once validated as safe for deployment with the radio network, the updates can be deployed for you by Motorola; or made available to you on Motorola's secure extranet site for implementation.

Rely on Motorola's certified security experts to identify and validate the necessary updates required to maintain cybersecurity readiness. Security Update Service ensures the right patches are identified, validated and applied in a timely manner to minimize cybersecurity risk and increase the operational integrity of your mission critical communications system.

CYBER ATTACKS

75% USED VULNERABILITIES THAT COULD BE PATCHED[1]

SECURITY BREACHES

73% ARE CAUSED BY MISCONFIGURATION OR USER ERROR

55% SECURITY INCIDENTS WERE CAUSED BY INTERNAL ACTORS[2]

MINIMIZE RISK AND COSTS

Security Update Service delivers:

Increased network availability
Reduce the vulnerabilities addressed by security patches and increase the safeguards of confidentiality, integrity, and availability of mission-critical systems.

Reduced maintenance costs
Dramatically reduce potential for system downtime; resulting in fewer maintenance costs to restore the system back to proper operational state.

Assurance
Motorola assumes responsibility to verify security updates without unnecessary burden to your staff.

Better use of technical resources
Keep staff focused on core responsibilities relying on Motorola to deliver the expertise and support for a proper cybersecurity regimen.

DELIVERY OPTIONS

One of the two options available for deploying security updates onto your radio network once software is pre-tested is included in our managed and support services packages.

Customer download
Included with our Essential Services, the latest security updates are made available via Motorola's secure extranet site for your team to download and install onto your radio network.

Remote SUS delivery
As an Advanced or Premier Services customer, Motorola's dedicated staff remotely installs the security updates onto your radio network. Vulnerabilities from third party software are addressed as soon as the validation of recommended patches is completed. We will also provide reports outlining updates made for your team's review and awareness.

SOURCE:
1. CSIS Raising The Bar for Cybersecurity Feb 2013
2. 2015 Verizon Wireless Data Breach Investigation Report

For more information about Security Update Service, contact your Motorola representative or visit motorolasolutions.com/cybersecurity.

MOTOROLA SOLUTIONS