SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

OT Cybersecurity Solutions for Implementation of IT-Sicherheitsgesetz 2.0

How Dragos Can Help German Organizations Meet and Exceed New Requirements

The mission of Dragos is to safeguard civilization by providing the platform, services, and intelligence to protect operational technology and critical infrastructure. Our technology supports numerous standards and regulations, empowering our customers to adopt best practices and exceed compliance requirements.

The German Bundestag adopted the IT Security Act 2.0 (IT-Sicherheitsgesetz 2.0 – "IT-SiG 2.0") in April, 2021. In May, the draft IT-SiG 2.0 was endorsed in the Bundesrat. This regulation provides amendments and updates to the original (IT-SiG 1.0), bringing a focus to the German Act to Strengthen the Security of Federal Information Technology (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSIG.)

Among the key updates, the role of the Federal Office for Information Security (Bundesamt für Informationssicherheit – BSI) has been elevated to a general authority for security in information technology and thus also as a national cybersecurity certification authority within the meaning of the EU Cybersecurity Act (Regulation (EU) 2019/881.) The BSI's powers to receive information on IT vulnerabilities and to notify affected IT manufacturers are expanded, and it is also clarified that the BSI is not entitled to refuse to accept information. The catalog of provisions on fines has been increased and provides more details for better enforcement. Instead of the fines of up to 100,000 EUR or up to 50,000 EUR possible under the previous BSI Act, administrative offenses can now – depending on the case – be punished with a fine of up to 2,000,000 EUR.

IT-Sicherheitsgesetz 2.0 aims for a more aligned cybersecurity management approach to mitigate inconsistencies in cybersecurity resilience across sectors, outlining several key measures to manage risks posed to networks and information systems.

The IT-Sicherheitsgesetz 2.0 strengthens the BSI in the following areas:

- **Detection and defense:** The BSI has received increased authorities in the detection of security vulnerabilities and the defense against cyber attacks. As Germany's primary competence center for information security, the BSI can thus shape secure digitalization and set binding minimum standards for the federal authorities and monitor them more effectively.
- **Cybersecurity in mobile networks:** The Act prohibits the use of critical components to protect public order or security in Germany. Network operators must meet specific high-level security requirements and critical components must be certified. The law also ensures information security in 5G mobile networks.
- **Consumer protection:** The BSI will be the independent, neutral advisory and protection body for consumers on IT security issues at the federal level. The introduction of the uniform IT Security Mark for citizens is intended to make IT security more transparent in the future and to make it clear which products already comply with specific IT security standards.
- **Security for businesses:** Critical infrastructure has been expanded to include the municipal waste management sector. In addition, other companies in the special public interest (for example, arms manufacturers, automotive manufacturers, or other companies of particularly high economic or strategic importance) will also have to implement certain IT security measures in the future and will be included in exchanges of confidential information with the BSI.
- **National Cybersecurity Certification Authority:** According to Section 9a (1), the BSI is the National Cybersecurity Certification Authority (NCCA) within the meaning of Article 58(1) of Regulation (EU) 2019/881, also known as the Cybersecurity Act (CSA). The NCCA is responsible for overseeing and enforcing rules as part of the European schemes for cybersecurity certification. The activities of supervision and certification are to be kept strictly discrete and carried out independently.

Which industrial sectors are covered by IT-Sicherheitsgesetz 2.0?

* Critical components are defined as IT products (i) that are used in critical infrastructures; (ii) for which disruptions to availability, integrity, authenticity and confidentiality may lead to a failure or a significant impairment of the functionality of critical infrastructures or to threats to public safety; and (iii) that on the basis of a law regarding this provision are designated as a critical component, or realize a function designated as critical on the basis of a law.

** Companies in the special public interest include companies that are not operators of critical infrastructures and (i) manufacture or develop defense products or IT products used in the processing of classified state information; or (ii) are among the largest companies in Germany (or critical suppliers to those companies) and are therefore of considerable economic importance; or (iii) operators of an upper-tier establishment within the meaning of the Hazardous Incident Ordinance (Störfall-Verordnung).

5 Critical Controls to Meet IT-Sicherheitsgesetz 2.0 Requirements

Dragos offers monitoring technology, threat intelligence, incident response, and professional services to help your organization meet and exceed the requirements of IT-Sicherheitsgesetz 2.0. We partner directly with CISOs and other leaders in your company to help you develop a vision, create a detailed action plan, and achieve consistent and documented results.

Dragos co-founder and CEO Robert M. Lee worked with SANS Institute ICS Curriculum Director Tim Conway to identify **5 Critical Controls for ICS/OT Cybersecurity**. These controls can be applied globally to enable organizations to meet and exceed several regulations, including IT-Sicherheitsgesetz 2.0. The five critical controls put a strong emphasis on practices that facilitate an active defense as opposed to a traditional prevention-focused approach, aligning well with the thought process behind IT-Sicherheitsgesetz 2.0.

CRITICAL CONTROL	SUMMARY OF CONTROL	IT-SICHERHEITSGESETZ 2.0 DIRECTIVE APPLICABILITY
ICS Incident Response Plan	Create a dedicated plan that includes the right points of contact, such as which employees have which skills inside which plant, as well as thought-out next steps for specific scenarios at specific locations. Identify responsible parties, notifications, and escalation policies. Leverage tabletop simulation exercises to test and improve response plans.	Obligation to release the information necessary to manage any disruption Incident handling (prevention, detection, and response to incidents) Business continuity and crisis management
Defensible Architecture	OT security strategies often start with hardening the environment - removing extraneous OT network access points, maintaining strong policy control at IT/OT interface points, and mitigating high risk vulnerabilities. Perhaps even more important than a secure architecture are the people and processes to maintain it. The resources and technical skills required to adapt to new vulnerabilities and threats should not be underestimated.	Obligation of operators of critical infrastructures to obtain supplier guarantees and notify the BMI of the planned first-time use of a critical component prior to its use Policies and procedures to assess the effectiveness of cybersecurity risk management measures Supply chain security – including security-related aspects of relationships between each entity and (i) its suppliers or (ii) service providers (such as data storage providers and processing services or managed security services providers)

CRITICAL CONTROL	SUMMARY OF CONTROL	IT-SICHERHEITSGESETZ 2.0 DIRECTIVE APPLICABILITY
ICS Network Visibility and Monitoring	A successful OT security posture maintains an inventory of assets, maps vulnerabilities against those assets (and mitigation plans), and actively monitors traffic for potential threats. Visibility gained from monitoring your industrial assets validates the security controls implemented in a defensible architecture. Threat detection from monitoring allows for scaling and automation for large and complex networks. Additionally, monitoring can also identify vulnerabilities easily for action.	Obligation to use attack detection systems Risk analysis and information system security policies
Secure Remote Access	Secure remote access is critical to OT environments. A key method, multi-factor authentication (MFA), is a rare case of a classic IT control that can be appropriately applied to OT. Implement MFA across your systems of systems to add an extra layer of security for a relatively small investment. Where MFA is not possible, consider alternate controls such as jump hosts with focused monitoring. The focus should be placed on connections in and out of the OT network and not on connections inside the network.	The use of cryptography and encryption
Risk-Based Vulnerability Management	Knowing your vulnerabilities – and having a plan to manage them – is a critical component to a defensible architecture. Over 1200 OT-specific vulnerabilities were released last year, most of them with incomplete or erroneous information. While patching an IT system like a worker's laptop is relatively easy, shutting down a plant has huge costs. An effective OT vulnerability management program requires timely awareness of key vulnerabilities that apply to the environment, with correct information and risk ratings, as well as alternative mitigation strategies to minimize exposure while continuing to operate.	Obligation to submit the documents required for an assessment from the point of view of the BSI and to provide the information Risk analysis and information system security policies Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosures

Next Steps: Get Aligned to the IT-Sicherheitsgesetz 2.0 Requirements

Dragos recommends working with your executive leadership and management teams to get all stakeholders involved in discussions about IT-Sicherheitsgesetz 2.0 compliance. Taking these steps now will ensure that your organization is ready to deploy programs and procedures that are compliant with the regulations.

STEP 1	Raise awareness among top management about cybersecurity risk management, the IT-Sicherheitsgesetz 2.0 requirements, and the potential impacts of maintaining the status quo.
STEP 2	Work with internal teams to review the cybersecurity risk management measures mandated by the IT-Sicherheitsgesetz 2.0. Identify how mature your organization is currently within each of the mandates.
STEP 3	Consider incident response and reporting first. Do you have a response retainer in place? Do you have a fully developed, agreed upon, and practiced incident response plan? Do you know what triggers the incident response process to begin? Does your organization have a business continuity and crisis management plan that integrates all areas of your business? If you say no to any of those questions, consider working with Dragos to get your incident response program fully developed and integrated into your processes.
STEP 4	Assess the security of your supply chain. You'll need a list of every asset that's part of your environment (made much easier by using technology like the Dragos Platform) – each of those asset vendors would be part of your supply chain. What software is being utilized throughout your process? Those vendors are part of your supply chain, too. Same goes for the hardware and software at the enterprise level because it is connected to your plant- and facility-level networks. All these vendors will need to be assessed and will need to provide you with security guarantees. Dragos can identify remote access connections used by third parties, evaluate the policies and controls used to manage that connectivity, and recommend changes to technologies, policies, and procedures to make that access more secure.
STEP 5	Create a full OT cybersecurity roadmap, complete with your current level of maturity in key areas and time-bound plans for improving and optimizing. From technology adoption to workforce development, you'll want to create a long-term view of your cyber readiness so that you can consistently measure progress.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.