baramundi

BARAMUNDI CHECKLISTS provide concise, step-by-step expert advice for handling common IT challenges in a straightforward way. You can find more checklists at: www.baramundi.com/checklists

The Challenges of Obtaining Cyber Insurance

For many underwriters, the field of cyber insurance is still relatively uncharted territory. With few generally applicable guidelines or requirements to follow, current and prospective policyholders should consider these points:

No binding standards

Insurance companies are currently orienting themselves e.g. to the standards of the NIST Cybersecurity Framework (National Institute of Standards and Technology) and ISO/IEC 27001. The insurance company is primarily wants to know: Does the company have its IT under control?

Inventory and reporting

An accurate and current inventory of all network devices is the essential starting point for identifying and assessing existing cybersecurity risks. Regular reporting provides the basis for establishing and maintaining coverage.

Take responsibility

Duty of care is key. This includes documenting practices for closing known vulnerabilities, regularly creating and testing backups, and other factors.

Legacy systems

Many insurance policies exclude damage caused by continued operation of legacy systems. This mainly affects industrial and manufacturing companies who must implement appropriate measures to protect older systems from malicious actors.

Raise awareness

Policyholders are responsible for training employees how to recognize and respond correctly to cyber threats. Most insurance companies reward or require recurrent cybersecurity awareness training.

Coverage expectations

Even in the event of an incident, the amount paid out rarely covers the entire loss. In most cases, 10 percent is reserved for the deployment of an incident response team to ensure rapid remediation and recovery after a major incident. Moreover, investing resources in prevention pays off better in case of doubt than relying solely on a policy.

The baramundi Management Suite (bMS) modules Inventory, OT Inventory, Network Devices, Mobile Devices Premium, Vulnerability Scanner, OT Vulnerability Identification, Patch Management, Managed Software, Device Control, Defense Control and Personal Backup and Disaster Recovery provide all capabilities needed to support cyber insurance coverage.