Cybersecurity in small and medium-sized enterprises: An overview of the solutions offered by Jawnet IT Services LTD

Jawnet IT Services protects small and medium-sized enterprises from cyber threats with tailor-made security solutions.

Jawnet IT Services LTD

MARSA, MALTA, July 20, 2026 /EINPresswire.com/ -- Alexander Jawinski and his team have implemented numerous security projects for companies of various sizes in recent years. Jawnet IT Services has gained experience with both international corporations and medium-sized companies. The projects included banks, industrial companies and government agencies, each of which required the highest security standards. In particular, the collaboration with financial service providers such as St.Galler Kantonalbank and Mizuho Finance Group demonstrates the company's expertise in the field of critical security infrastructures.

Why cybersecurity has become so important for SMEs

In the past, many small and medium-sized enterprises thought, "Who would attack us?" Those days are definitely over. Today, small and medium-sized enterprises are popular targets for cybercriminals – they often have less protection than large corporations, but still have valuable data and money.

The threat landscape has changed dramatically. Ransomware attacks, in which data is encrypted and a ransom is demanded, affect German companies on a daily basis. Phishing emails are becoming increasingly sophisticated and are almost indistinguishable from genuine messages. In addition, there are targeted attacks on vulnerabilities in outdated software or insecure remote access.

What makes this particularly treacherous is that many attacks remain undetected for months. During this time, criminals spy on data, collect information about business partners or prepare larger attacks. The financial damage often runs into the hundreds of thousands, not to mention the damage to reputation.

Typical vulnerabilities in small and medium-sized businesses

SMEs often have similar security gaps that pave the way for attackers to enter the company network:

- Outdated software without the latest security updates
- Weak or reused passwords for critical systems
- Missing or untested backup strategies
- Untrained employees with no security awareness
- Insecure remote access for home offices or external service providers
- Firewalls with outdated configurations from the time of installation

Many still use Windows systems that are no longer supported or have not updated their network components for years. Jawnet IT Services LTD identifies such vulnerabilities through systematic security audits and develops appropriate countermeasures.

Jawnet IT Services: Holistic approach to security

Security is not a product that you buy once and then forget about. It is an ongoing process that requires regular maintenance. That is why Jawnet IT Services takes a holistic approach that considers both the technology and the people in the company.

Network security as the foundation

The network is the backbone of any IT infrastructure – and usually the first point of attack for criminals. That's why every security strategy starts with a solid network architecture. Latest-generation firewalls, intrusion detection systems and segmented networks create multiple layers of security.

When configuring network components for customers such as Braskem Europe or various government agencies, security has always been the focus. VPN connections between locations are encrypted, access is strictly controlled and suspicious activity is detected immediately.

The correct configuration of VLANs is particularly important. This allows different areas of the company to be separated from each other – if one area is compromised, an attacker cannot spread unhindered throughout the entire network. The validation of private VLANs and IP

configurations is one of our standard services.

Endpoint security for all devices

Every computer, tablet and smartphone can be a gateway for attackers. That's why every device that connects to the company network needs appropriate protection. Modern endpoint protection solutions go far beyond traditional antivirus programmes.

They detect suspicious behaviour patterns, block malicious websites and control which programmes are allowed to run. Particularly when setting up workstations, great importance is attached to the correct security configuration – from the initial installation to the latest software update.

Mobile device management is becoming increasingly important as employees increasingly use private devices for business purposes. Here, it is important to find the balance between security and user-friendliness so that the solutions are actually accepted and used.

Specific security solutions in detail

Security requirements vary depending on the industry and size of the company. A tax advisor needs different protective measures than a doctor's office or a mechanical engineering company. That is why there is no standard solution that fits all.

Backup and disaster recovery

When all protective measures fail, a functioning backup is often the last resort. But many companies make serious mistakes here: they don't test their backups, don't store them securely or forget important data. Alexander Jawinski has seen in various projects how quickly companies can find themselves in existential difficulties after a data loss.

A well-thought-out backup strategy follows the 3-2-1 rule: three copies of the data, on two different media, with one copy stored separately. But that is no longer enough today – backups must also be protected against encryption attacks.

Proven elements of a modern backup strategy include:

- Immutable backups that cannot be encrypted, even in the event of ransomware attacks
- Automated daily backups of all critical systems and data
- Regular restore tests to verify recoverability
- Geographically separate storage in case of natural disasters or fires
- Versioning for restoring files from different points in time

Jawnet IT Services integrates backup solutions as early as the planning phase of new IT infrastructures and ensures that everything works smoothly in an emergency.

Access control and authorisation management

Not every employee needs access to all data and systems. The principle of least privilege states that everyone should only have access to what they actually need for their work. This sounds simple, but it is often complicated to implement in practice.

Active Directory implementations and authorisation concepts are among the core competencies for larger installations. This involves not only one-time setup, but also ongoing maintenance – when employees leave the company or take on new tasks.

Two-factor authentication is becoming standard, especially for administrators and access to critical systems. What used to be considered a nuisance has now become indispensable.

Practical implementation for SMEs

Theory is one thing, practice is another. Many security solutions fail not because of the technology, but because of their implementation in everyday business life. Employees circumvent security measures if they are perceived as too complicated. Or there is a lack of know-how for proper configuration and maintenance.

Employee training as an important building block

The best protection is useless if an employee clicks on a phishing link or sticks their password on their monitor. That's why raising awareness among the workforce is part of any security strategy. This doesn't have to be a dry seminar – interactive training and regular tests often show better results.

It is also important to create a security culture in which employees can express concerns without fear of reprisals. Anyone who has accidentally clicked on a suspicious email should be able to report it so that a quick response can be made.

Monitoring and incident response

Attacks happen – the question is not if, but when. That's why every company needs a plan for how to respond in an emergency. Who is responsible? Which systems are shut down first? How are customers and partners informed?

24/7 monitoring often detects threats before major damage occurs. Automated systems can block suspicious activity and trigger alarms at the same time. In critical incidents, a quick

response is crucial – every minute can make the difference between a minor incident and major damage.

Outlook: Security in a connected world

The threat landscape is constantly evolving. What is secure today may be obsolete tomorrow. Cloud services, the Internet of Things and artificial intelligence bring new opportunities, but also new risks.

Successful cybersecurity in small and medium-sized businesses therefore requires partners such as Jawnet IT Services, who not only know the current threats but also keep an eye on future developments. Regular security audits, continuous training and adaptation of protective measures are essential.

Investing in IT security is not a cost centre, but insurance for the future of the company. Because one thing is certain: the attackers will not stop – but with the right measures, they can be successfully repelled.

Alexander Jawinski
Jawnet IT Services Ltd
OYIA Building, Level 2
MARSA CROSS ROAD
Marsa MRS1547
Malta
Phone: +356 79037561
Imprint: https://www.jawnet-it.com/imprint/

Alexander Jawinski
Jawnet IT Services
email us here