Reading Sample: Cyber Security Report 2026

Strategic Priorities for Small and Medium-Sized Enterprises (SMEs)

An exclusive insight into the key findings of the latest security report.

---

1. Executive Summary: The New Threat Landscape

The threat landscape for small and medium-sized enterprises (SMEs) has fundamentally shifted in 2026. Attackers are increasingly relying on identity-based attacks. This means they are no longer "breaking in" with traditional malware, but instead "logging in" with stolen, yet legitimate credentials. This trend is massively accelerated by AI-powered automation, such as deepfake phishing, and the targeted exploitation of browser vulnerabilities.

For SMEs in Germany, the implementation of the NIS-2 Directive at the start of 2026 has become a key regulatory driver. Companies that fail to invest in securing identities and hardening the browser as the primary work tool risk not only data loss but also significant business interruption. Current analyses indicate that such incidents now account for over 50% of the total costs associated with ransomware events.

2. Focus Area: Browser Security & Web-Based Attacks

Why the Browser Is the Primary Target in 2026

The web browser has become the primary entry point for attacks. This is mainly due to SMEs' increasing reliance on SaaS (Software as a Service) solutions such as Microsoft 365, Salesforce, and similar platforms. Attackers are focusing on compromising the browser session to gain direct access to corporate data, without having to attack the underlying operating system.

Current Attack Scenarios at a Glance

The following table illustrates the most common and dangerous attack methods currently targeting browsers and web-based sessions:

Scenario	How It Works	Practical Example
Quishing (QR Code Phishing)	Attackers send PDF invoices containing QR codes that link to malicious websites.	An employee scans a QR code on a supposed supplier invoice and enters their credentials there.
AiTM (Adversary-in-the-Middle)	Proxy servers intercept passwords and session tokens in real time.	An attacker takes over an active Microsoft 365 session even though Multi-Factor Authentication (MFA) is enabled.
Browser-Based Data Theft	Infostealer malware extracts stored passwords and cookies directly from the browser.	A personal device is infected, thereby exposing credentials for corporate accounts.

Recommended Actions

To effectively counter these threats, companies must take proactive measures. A strict separation of personal and business use is essential to prevent cross-contamination from personal devices. This can be achieved by using virtual desktops or container solutions for the browser.

Furthermore, QR codes in email attachments and PDFs should be blocked by gateway filters to nip quishing attacks in the bud. Regular and enforced browser updates are mandatory to close known security vulnerabilities promptly. For enhanced protection against drive-by downloads and malware, the use of cloud-based browser isolation (e.g., Citrix Secure Browser) is also recommended.

> *"Identity is the only perimeter that holds in a cloud-first world. Protect access, not the network."*

Would you like to read the full report? The complete "Cyber Security Report 2026" contains further detailed analyses on modernizing the MFA strategy, Identity Risk & Access Management, and a concrete action plan for SMEs.