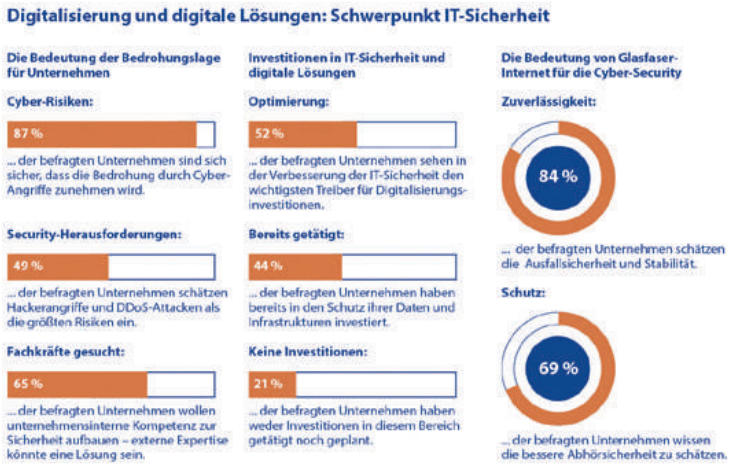
CYBER-RESILIENZ:

Wie Glasfaser mittelständische Unternehmen **schützt**

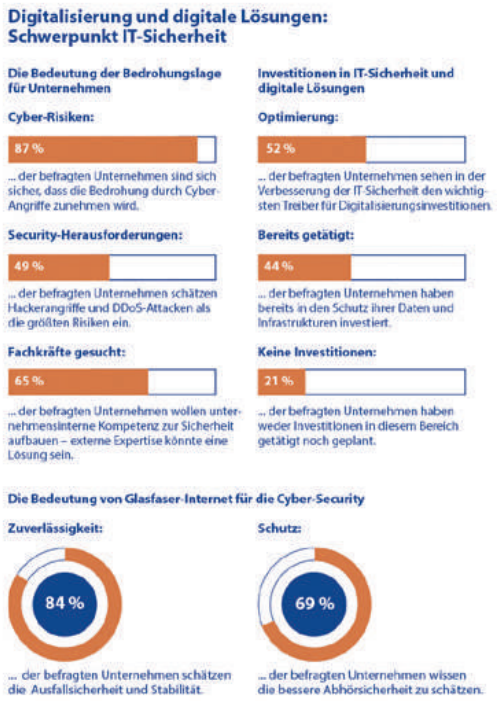
Die Digitalisierung eröffnet dem Handwerk neue Chancen, doch in einem heterogenen Umfeld mit vielen verschiedenen digitalen Systemen, Anwendungen und Endgeräten steigen auch die Cyberrisiken. Gerade in einer Branche, in der Vertrauen und Kundennähe essentiell sind, können Sicherheitslücken weitreichende Konsequenzen haben. Eine Architektur aus moderner Glasfaser-Infrastruktur und Sicherheitslösungen, die zentral im Netz dauerhaft mitlaufen, bilden das Fundament für eine sichere und zukunftsfähige IT … | VON FRANK ROSENBERGER

Ob digitale Angebotserstellung, vernetztes Personalmanagement oder der Einsatz KI-gestützter Tools: Die Digitalisierung hat das Handwerk längst erreicht und macht viele Abläufe effizienter und kundenfreundlicher. Doch gleichzeitig gewinnt ein bewußter Umgang mit IT-Sicherheit an Bedeutung, um diese Chancen zu nutzen und sich gegen Cyberbedrohungen zu wappnen. Phishing-Mails, Ransomware und DDoS-Angriffe treffen immer häufiger auch kleine und mittelständische Betriebe – oft, weil es hier an ausreichenden IT-Schutzmechanismen, Expertise oder moderner Infrastruktur mangelt. Besonders gefährdet sind unzureichend gesicherte Kundendaten und mobile Geräte – etwa durch veraltete Software oder unsichere WLAN-Verbindungen. In heterogenen IT-Umfeldern, wie wir sie häufig im Handwerk vorfinden, sind netzbasierte Sicherheitslösungen die erste Wahl zur Erhöhung des Schutzlevels ohne kostenintensive Upgrades der Kundenhardware oder Systeme.



Laut einer YouGov-Studie im Auftrag von 1&1 Versatel* betrachten 87 % der befragten Unternehmen Cyberangriffe als zunehmende Bedrohung. Und das zu Recht: Mit über 20,5 Millionen DDoS-Attacken wurde im ersten Quartal 2025 im Vergleich zum Vorjahr ein neuer Höchstwert erreicht, wie der Cloudflare DDoS Threat Report zeigt. Oberflächliche Maßnahmen, z. B. zusätzliche Passwörter, gelegentliche Updates oder punktuelle Firewalls bieten keinen ausreichenden Schutz. Gefragt sind moderne und sichere Netzwerk-Infrastrukturen.

Bilder: 1&1 Versatel



Moderne Glasfaser-Infrastruktur als Fundament für IT-Sicherheit

Wer IT-Sicherheit ganzheitlich denkt, darf die physische Netzwerkanbindung nicht nachrangig behandeln. Nur wenn das Fundament stimmt, greifen Schutzmaßnahmen zuverlässig. Sie ist die Grundlage für stabile, ausfallsichere und abhörgeschützte Netzwerke. Im Vergleich zu Kupferkabeln ist Glasfaser unempfindlicher gegenüber elektromagnetischen Störungen, was die Ausfallsicherheit und die Verfügbarkeit kritischer Systeme erhöht. Eine leistungsfähige Glasfaser-Infrastruktur spielt auch bei der Abwehr moderner Cyberangriffe, etwa DDoS-Attacken, eine zentrale Rolle. Dabei versuchen Angreifer, Webserver, Online-Plattformen oder Cloud-Dienste durch eine Flut massenhafter Anfragen zu überlasten und lahmzulegen. Glasfaseranschlüsse sind durch ihre hohe Leistungsfähigkeit eine wichtige Grundlage für stabile und widerstandsfähige Netzwerke. In Kombination mit entsprechenden

Cyberbedrohungen im Überblick

- Phishing-Mails sind betrügerische E-Mails, die gezielt darauf abzielen, sensible Daten wie Passwörter, Kundendaten oder Bankinformationen zu stehlen. Im Handwerk können solche Mails beispielsweise als vermeintliche Rechnungen von Zulieferern oder Anfragen von Kunden getarnt sein.

- Ransomware ist eine Schadsoftware, die wichtige Betriebsdaten oder ganze IT-Systeme verschlüsselt und so den Arbeitsalltag lahmlegt. Im Handwerk betrifft dies oft Planungssoftware, digitale Auftragsmanagementsysteme oder Kundenkommunikation. Die Angreifer fordern ein Lösegeld, um die Daten wieder freizugeben.

- Bei einem Distributed-Denial-of-Service-(DDoS)-Angriff werden ein Webserver oder eine Online-Plattform durch die massive Überflutung mit Anfragen außer Betrieb gesetzt. Für Handwerksbetriebe bedeutet dies, daß Webseiten, Online-Terminbuchungssysteme oder digitale Angebotsplattformen plötzlich nicht mehr erreichbar sind.

netzbasierten Schutzmechanismen kann dies auch im Fall von DDoS-Angriffen hilfreich sein, um die Erreichbarkeit digitaler Dienste länger aufrechtzuerhalten.

Ganzheitliche IT-Sicherheit braucht den richtigen Dienstleister

Für Handwerksbetriebe ist die Wahl des richtigen Telekommunikationspartners ein zentraler Erfolgsfaktor. Neben Erfahrung und fairen Preisen kommt es darauf an, daß der Anbieter die IT-Sicherheit ganzheitlich abdeckt – also nicht nur Technik liefert, sondern auch weiß, wie man Betriebe im Alltag schützt und hilft, Mitarbeiter für die IT-Sicherheit zu sensibilisieren. Ein verläßlicher Partner betreibt ein eigenes Sicherheitszentrum und bietet alles aus einer Hand – von der Absicherung des Internetzugangs über das Erkennen von Angriffen bis hin zur Beratung bei Sicherheitsfragen und gesetzlichen Vorgaben. Wichtig ist auch, daß sich die Lösungen einfach in die vorhandene IT-Struktur einfügen, ohne den Betrieb zu stören. <<

Über den Autor

Frank Rosenberger ist seit Januar 2024 CEO von 1&1 Versatel, dem führenden Glasfaserspezialisten für Firmenkunden. Seine Leidenschaft für IT, digitale Transformation und Cybersicherheit treibt ihn an, Unternehmen mit sicheren und innovativen Lösungen in eine erfolgreiche digitale Zukunft zu führen.

** Zur Studie: https://www.1und1.net/sites/default/files/documents/pdf/1und1-versatel-studie-digitalisierungsbedarfe-von-unternehmen-0424.pdf*