HERMES CLOUD
MANAGED IT SERVICES

VOLUME 001 • APRIL 2026
AMSTERDAM, THE NETHERLANDS

TECH TALK

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE

STOP RANSOMWARE ---------- P1
ZERO-TRUST ROADMAP ---------- P2
SHADOW AI AUDIT ---------- P2
MISSING SECURITY LAYERS ---------- P2
TECHNOLOGY TRIVIA P2 ---------- P2

STOP RANSOMWARE IN ITS TRACKS: A 5-STEP PROACTIVE DEFENSE PLAN

Ransomware isn't a jump scare. It's a slow build

In many cases, it begins days, or even weeks, before encryption, with something mundane, like a login that never should have succeeded. That's why an effective ransomware defense plan is about more than deploying antimalware. It's about preventing unauthorized access from gaining traction.

Here's a five-step approach you can implement across small-business environments without turning security into a daily obstacle course.

THE 5-STEP RANSOMWARE DEFENSE PLAN

Each step is practical, MSP-friendly, and repeatable across small-business environments.

01 PHISHING-RESISTANT SIGN-INS
Authentication methods that can't be easily compromised. Enforce strong MFA across all accounts, with priority to admin and remote access infrastructure.

02 LEAST PRIVILEGE+ SEPARATION
Each account gets only the access it needs. Keep administrative accounts separate from everyday user accounts. Eliminate shared logins.

03 CLOSE KNOWN HOLES
Vulnerabilities attackers already know how to exploit. Set clear patch guidelines and prioritize internet-facing systems.

04 EARLY DETECTION
Identifying warning signs before encryption spreads. Includes endpoint monitoring and rules for immediate escalation vs review.

05 SECURE, TESTED BACKUPS
Backups that attackers can't easily access. Keep at least one copy isolated from the main environment. Run restore drills on a schedule.

REMCO HERMES
OWNER

We're passionate about making technology work for you. Let's have a quick, friendly chat to see how we can enhance your IT and keep your data secure. Contact us today to schedule a consultation.

ROADMAP FOR ZERO-TRUST ARCHITECTURE

Most small businesses aren't breached because they have no security. They're breached because a single stolen password becomes a master key.

Zero-trust architecture represents the shift that breaks that chain reaction. It treats every access request as potentially risky and requires verification every time.

"NEVER TRUST, ALWAYS VERIFY."

3 CORE PRINCIPLES

IDENTITY-FIRST CONTROLS:
Strong MFA, blocking risky legacy authentication, and applying stricter policies to admin accounts.

DEVICE-AWARE ACCESS:
Evaluating who is signing in and whether their device is managed, patched, and meets your standards.

SEGMENTATION TO LIMIT IMPACT:
Breaking your environment into smaller zones so access to one area doesn't automatically grant access.

SHADOW AI AUDIT

Shadow AI is the unsanctioned use of AI tools without IT approval. 38% of employees admit they've shared sensitive info without permission. The goal isn't to block AI, but to prevent data exposure

"We'll help you gain visibility and put guardrails in place without slowing yourteam down."

LAPTOPS AT HOME CHECKLIST

- LOCK SCREEN EVERY TIME YOU STEP AWAY
- STORE WORK LAPTOPS SECURELY WHEN NOT IN USE
- DON'T SHARE WITH FAMILY MEMBERS OR GUESTS
- USE STRONG SIGN-INS AND MFA ON WORK ACCOUNTS
- PATCH FAST: ENABLE AUTOMATIC UPDATES
- SECURE HOME WI-FI LIKE IT'S PART OF THE OFFICE

5 MISSING SECURITY LAYERS (AND HOW TO ADD THEM)

01 PHISHING-RESISTANT AUTHENTICATION
Enforce strong MFA everywhere, then tighten admin and remote access first.

02 DEVICETRUST AND USAGEPOLICIES
Define what a compliant device is, and what happens when it isn't

03 EMAIL AND USER RISK CONTROLS
Reduce exposure by default with filtering, warnings, and easy reporting

04 CONTINUOUS VULNERABILITY COVERAGE
Measure patch latency and include third-party apps in your stack.

05 PROVEN RECOVERY & RESTOREDRILLS
Run restore drills and define recovery priorities before you need them.

"Turn your business security into a repeatable, measurable baseline."

TECHNOLOGY TRIVIA QUESTION

Win a $50 Amazon Gift Voucher by being the first person to email us the correct answer!

WHAT IS THE TYPE OF MALWARE THAT DISGUISES ITSELF AS LEGITIMATE OR USEFUL SOFTWARE?

LAST MONTH'S ANSWER:
Ada Lovelace

Email info@hermescloud.nl to win!

amazon
$50 GIFT CARD