Ransomware protection checklist

- [ ] At least one copy of critical data cannot be deleted from the working network, even with admin rights.
- [ ] In the last quarter you restored at least one critical system from backup and recorded how many hours it took.
- [ ] MFA is on for everyone in email, VPN and cloud admin panels, with no exceptions for managers.
- [ ] RDP and other remote access services are not exposed directly to the internet.
- [ ] Edge devices (VPN, firewall, router) run current firmware, and one person is responsible for it.
- [ ] Only those who need admin rights have them, and admin work is done from separate accounts.
- [ ] Staff know where to report a suspicious email, and this has been tested with a phishing simulation.
- [ ] The response plan with phone numbers for your IT provider, lawyer, police and national CERT is printed.
- [ ] Your IT provider's access is known, limited and protected with MFA.

Want to go through this checklist together? Write to us and we will review your scope.
veiltrack.io/en/contact