| **Step** | **Domain** | **Minimum Acceptable Level** | **Findings** |
| --- | --- | --- | --- |
|  | Digital Identities | * Directory Services or any kind are used. * Unique IDs are used * Permissions are assigned via Groups in the Directory Service * Service and Cloud accounts are gathered, minimized, and under control | * Acquisition Target is a 24 people company – started circa 15 years ago. * Microsoft Small Business 2008 Premium with AD. * 10 groups used to ERP and TS – shared mailboxes of 3-4 persons for orders using AD groups * Spam filtering and GFI managed AV are the only Cloud services used (maybe email marketing campaign) * TBD: provision Corporate File Sharing Solution |
|  | Admin Accounts | * Admin accounts are managed under a Directory Service * Admin accounts are unique for each admin * Central ownership of who gets appropriate rights * Process for removing rights as appropriate | * Quality manager – ISO 9001 currently not kept, but should be easy to renew. * No privacy officer (this country does not require one by law) * 4 service accounts – Administrators, personal account as admin, support admins (Outsourced Hosting), sync user for the old ERP software (phased out) Admin in AD and Exchange – 3 or 4 months to phase out (first of May) * Leavers are rare, there is no written process, but when this happens they are quickly removed from AD (last day of work) |
|  | Endpoints / Client Systems | * Client types are reduced as much as possible * Disk encryption is applied, especially for mobile computers * Security patches on clients are applied at least monthly * There is a procedure to update software at least quarterly, or after major releases * AV from a reputable vendor, and signatures are updated at least daily * Secure procedure is for software updates and new software defined | * Windows 7 is the standard. Tinkering with Windows 10 * XYZ Anti-Virus (Cloud Based) – WXY antivirus was in place previously but has shown to not be good enough * Central firewall is Grandiose Firewall Brand Model 123 with Intrusion Detection license in the office. 1.000 € with no license – security license 1.000 € / years – expiration middle March * 3-4 persons with 4G dongles. * Other people (how many?) uses Grandiose Firewall Home Edition – 335€ license – no license for Intrusion Detection at home * Rare VPN software client on the laptop – VPN licenses from Grandiose Brand, but looking into Another Brand because of Windows 10 support. * Split horizon of people using VPN from home. * Company pays Internet connection (fiber) for home, but administrative hassle, therefore looked into 4G dongles. * People working from home use RDP to access the Terminal Services (TS) in the office * 10 users circa simultaneous connection, of which 5 from home; 1 from abroad – 3/4 from 4G * Admin rights are used on laptops, but not on TS, although some users managed to have DropBox working on TS too! * Kind of “gold” image for laptops is used, but it is difficult as there are three kinds of laptops: Dell, HP and Lenovo. * Windows Update is let run loose on clients, but people have admin rights so they can override it. * TBD: setup a Phishing exercise to understand user awareness * IT to provide temporary VPN access to employees who need access to corporate networks. Access at the moment to be limited to OWA and SharePoint (web access). * Define timeframe by which employees will need to migrate Target clients to Corporate standards. |
|  | Servers | * Minimum level of physical restriction are applied to server access * There is an AV from a reputable vendor, and signatures are updated at least daily * Software installation and updates must have a secure procedure * Central rules for security controls and priorities | * Server room of Target is shared with another company present in the same building. By May, the second firm will move out, and a plan to export data for them has to be conceived. * At least once a month Microsoft patches are applied on servers’ VMs as required. * AV is provided by XYZ AV, which has Cloud update for AV signatures and has proven to be better than previous AV. * There is the possibility to also install a secondary AV along the first one. |
|  | Networks | * Secure connectivity between ResMed and target * Secure access from Target staff and stakeholders * Periodic security controls review for compliance | * 3 different fiber connections come into the building   + BackOffice – owner of the building has one fiber – used for guest wireless LAN and meeting room   + Main fiber 24x7 support – only for corporate main internet access – WAN   + Backup Internet fiber – WAN – cheaper – connected to Grandiose Firewall Brand. * IP address list available * Subnet restrictions on computer coming in for site-to-site VPN and DHCP. No VLANs are used as they are overkill here. * 2 IP addresses exposed on the Internet * 1 IP address whitelisted from Outsourced Hosting provider which can only get to 1 TS for store, packaging – not so critical – they can connect to SQL Servers VMs for support * Second IP is not used – only for tests etc. |
|  | Hosting | Minimal controls include:   * contract controls * confirmation of hosting partners security controls * Policies for Target hosting and cloud usage * Security controls to protect / encrypt co-hosted data | * Two racks data room. * ERP: Microsoft Dynamics C5 hosted on premise * CRM: Microsoft Dynamics CRM hosted at Outsourced Hosting Data Center. * (Old CRM: Superoffice to be retired in 12/2015) * Web site with web shop: www.xyz.com hosted at My Outsourced Hosting Provider, Inc. * Kind of SQL Loader from ERP to hosting – Outsourced Hosting DC does this via RDP to the MS SQL Server 2008 or the MS C5 to update or program the ERP. * Outsourced hosting and Target Company to setup VPN connection. Management is performed via Teamviewer. A jump host is to be setup between the two parties. |
|  | Email | * Email use policy in place * User awareness for email security and anti-phishing * Tools and processes for anti-phishing, malware and anti-spam | * 15 minutes awareness on IT and Security done during the monthly all-hands meeting. * XYZ Cloud anti-spam and anti-phishing is used for email * Problem of separation between private and business in the past. * Marketing using LinkedIn and Facebook. Email marketing not known which tool. * External company used as email relay – to be received * TBD: IT policy in local language – to be received * TBD: setup a Phishing exercise to understand user awareness |
|  | Data Recovery | * Proven data backup / recovery capabilities * Testing of solutions * Viable DR plan | * Backups on 2 NAS drives + 1 tape drive. 1 weekly backup on tape, daily backup on NAS on different location in the same building. 2 QNAPs, one in the server room and one in the cleaning room (which can be locked). Symantec Backup Exec (VERITAS). * One NAS is located into a cleaning room; it is to be moved and/or secured with a proper rack and ventilation. * No DR concept. Most important is the ERP. * Cloud backups have been discarded as they may not guarantee lawful data residency. * An offer for offsite backup to Outsourced Hosting is requested. |
|  | Boundary Defenses | Firewalls  Next-Generation Firewalls, Proxies  URL filtering  VPN concentrators  Site-to-Site VPNs  Use of encryption  Web Application Firewalls  DoS/DDoS protection | * 2 IP addresses exposed on the Internet * 1 IP address whitelisted from Outsourced Hosting which can only get to 1 TS for store, packaging – not so critical – they can connect to SQL Servers VMs for support * Second IP is not used – only for tests etc. * TBD: email relay company – reference to be provided * VPN concentrator from Grandiose Firewall Brand. SSLVPN does not work with Outsourced Hosting. * Anti-malware service provided as Intrusion Detection subscription with Grandiose Firewall. * No encryption on laptops, however there is very little data due to massive use of TS. * No DDoS or WAF protection. Web Shop does not have advanced security. SSL implemented recently for the whole site. Security issues are managed/responsibility is to Outsourced Hosting. The web shop is an implementation of some off-the-shelf e-commerce product from Outsourced Hosting. * No direct connection between ERP and web shop. Orders arrive via email to the ordering team which processes them. In this country, all commercial transactions require electronic registration by the Ministry of Commerce; this is performed automatically by the e-commerce software. This guarantees against missing payment of orders and does not require the e-shop to process or store credit cards or other financial transactions. * Registration of customers in the web shop is not compulsory to purchase products; however, as mentioned, electronic registration of invoices is mandatory in this country. * Payment information are processed by the ordering personnel and the invoice number ID is stored in the ERP. |
|  | Inventory | Full asset inventory  Network diagram | * Asset inventory – only laptops – Samsung screen with XP embedded doing RDP. Not very useful or maintained. * TBD: Network Diagram with Security/Network Engineering. |
|  | Operational Security | Hiring processes  Log management and review  Monitoring processes and capabilities  Multi-Factor authentication  Periodic vulnerability assessments and pen tests  Process for mitigating critical findings  Encryption of mobile systems and sensitive data in systems  Tested and periodically updated incident response plan | * External IT Security firm has been called for local assessment 8 years ago, and then again 3 years ago. Findings about password policy which has been forced to update password every 6 months which has disgruntled users slightly. * Once a week log reviews done generally on Sunday, to observe if urgent work is due on Monday. * XYZ Firewall dashboard has monitoring – if it cannot get to the server gets an alarm – TBD: get some screenshot of XYZ dashboard. * No Multi-factors or steps for authentication. * TBD: get screenshots of AD with password policy, groups, etc. * There is no vulnerability management and patch management process for clients (servers are manually patched as required once a month) * There is no periodic test or incident response plan |
|  | Physical | * Physical Security plan * Access control systems * Critical/High Impact IT infrastructure is physically segregated * Physical access is logged/monitored | * Server room is shared with another company in the same building. * Other firm and Target are on the same server. By May the Other Firm will move out, and a plan to export data for them has to be conceived. * Facility Firm rent out offices downstairs. They have access to server room, internet, routing and telephone system connections to another country via VPN. * Door locked, Facility Firm does not come often. * One of the Backup NAS is in a cleaning room; door is locked, technically cleaning lady can steal backups. * On site verification of physical access limitation suggested. |
|  | Wireless | * Wireless segregated from Critical/High Impact IT infrastructure * Wi-Fi corporate and guest * Wi-Fi monitoring * Wi-Fi access control | * Wi-Fi AP from Grandiose Brand are not good; older Grandiose Brand Wireless models are used a Guest Wi-Fi * Corporate Wi-Fi is provided by Less Grandiose business AP; centralized configuration with 1 master and 3 slaves * There is one Less Grandiose user password; users use this to get into the corporate Wi-Fi * There is no MDM used, no control of wireless devices. * On site wireless survey suggested. * Implement MDM/802.1x with Corporate standard. |