Übung: Planung einer sicheren IT-Infrastruktur für Unternehmen X

Unternehmen X vertreten durch den „IT-Beauftragten Knopper“, der die Fakten seines Unternehmens kennt, was die IT angeht. *„Wir verkaufen ein sicherheitskritisches Produkt und wollen in der Firma keine Malware oder Spionage.“*

Beratendes IT-Consulting Unternehmen: Sie. :-)

1 Vorgehen?

Fragenkatalog, um festzustellen, worum es geht, und was Unternehmen X BRAUCHT!

1. Wie viele Standort? Einer.
2. Gastzugänge? Ja, gelegentlich kommen Kunden vorbei, bringen Geräte mit und lassen sich bei der Konfiguration helfen, gehen auch bei uns ins Internet.
3. Gibt es eine Firmen-Webseite? Ja.
4. Gibt es Intranet? Es gibt in der Firma ein internes Netz, von dem aus kommen wir auch ins Internet.
5. Mitarbeiteranzahl? 10, sitzen auch alle am Standort
6. Hat jeder Internetzugang? Ja.
7. Braucht jeder Internetzugang? (Mitarbeiter rufen: „JA!!!“)
8. Gibt es eine Firewall? Wir haben einen Router ins Internet
9. Welche Betriebssysteme werden verwendet? Einige Mitarbeiter haben Linux, andere Mac, andere Windows, Smartphones und Tablets sowohl Android als auch IOS.
10. Gibt es einen Server? Wir haben einen Intranet-Server und einen Webserver, letzterer ist auch von außen erreichbar. Beide laufen auf dem Rechner, der uns auch Internet-Zugang zur Verfügung stellt.
11. Was ist Ihr Produkt? „Smart Networks“ stellt WLAN-steuerbare Funksteckdosen her, die sowohl lokal (per Browser) oder Remote (per App oder auch Browser) gesteuert werden können. Diese Messen auch Stromverbrauch und Temperatur, was mit der App als Statistik darstellen. Auch per Sprache durch Alexa und Co steuerbar, evtl. später auch mit Kommunikationsfunktion.
12. Ist die Konfiguration der Funkteckdose Passwortgeschützt? Selbstverständlich, das Passwort wird bei der Initialkonfiguration der Funksteckdose gesetzt.

13. Gibt es einen Proxy, über den die Funksteckdose vom Anwender gesteuert wird bzw. für Updates? Ja, beides, der läuft auch auf unserem Firewall.
14. Wie sieht das aktuelle Netz aus?
15. Alle Dienste auf einem Server? Ja, das ist sehr praktisch. Eine Stelle zum Administrieren.
16. Was ist das Problem? Vor ein Paar Wochen gab es eine erfolgreiche Malware-Attacke auf die Windows-Rechner im Netz. Wir wissen nicht, die reinkamen. Wir wollen, dass so etwas nicht mehr passieren kann. Bei der Gelegenheit sollten natürlich auch andere mögliche Sicherheitslücken behoben werden.
17. Budget? So viel wie wir ausgeben müssen, um sicher zu sein, und wir uns leisten können.
18. Ist mit Widerstand zu rechnen, wenn Schutzmaßnahmen implementiert werden? (Stimme aus dem Off: „Ja!“) Chef sagt „nein“.
19. Können die Mitarbeiter das Netz auch privat nutzen? Klares „Ja“, wir wollen, dass sich die Mitarbeiter am Arbeitsplatz wohl fühlen, und so lange es sich freiwillig auf ein gesundes Maß begrenzt, darf jeder auch privat Mail lesen, Streamen, auf ebay einkaufen usw.
20. Ist Internetzugang und die Nutzung aller Dienste aus internem UND Gastnetz möglich? Ja.
21. Wäre Outsourcing denkbar, z.B. die Webseite? Kommt nicht in Frage, wir möchten die komplette Kontrolle über unseren Webserver.
22. Wie viele Mitarbeiter brauchen Zugriff auf den Webserver? 4 von den 10
23. Was wird bereits bezüglich Verschlüsselung etc getan? Der Webserver hat ein SSL-Zertifikat (nur https erlaubt), man kommt per SSH an den Server zur Wartung (von innen und außen nur mit Passwort), WLAN ist WPA-Verschlüsselt, ansonsten fällt mir nichts ein.
24. Müssen Dienste von außen gewartet werden? Nein.

2 Überlegungen…

Was sollte man ändern und warum?

1. Wie viele Netzwerke brauchen wir? Sinnvoll: 3 oder 4
   1. Intranet
   2. Gastzugang Besucher
   3. DMZ für extern angebotene Dienste WWW und App-Server (Steckdosen) und DB
   hier: 1 Rechner für externe Dienste, VMs für einzelne Programme mit Möglichkeit, vom WWW und App-Server auf DB zuzugreifen.

2. Mailserver in Sandwich-Konfiguration (Filter) in Intranet mit Port-Forwarding vom Firewall,
3. Regelmäßige Checks der Geräte im Intranet
4. Sicherheits-Policy (Richtlinien) für Mitarbeiter:
   Bitte nur Geräte mitbringen, bei denen man regelmäßig auf Schadsoftware geprüft hat.

Verschlüsselung verwenden
Keine ungeprüfte Software installieren / starten
(ggf. Schulung)

5. Accesspoints so konfigurieren, dass sie Verbindungen zu bekannten Malware-Sites erkennen, melden und unterbinden.
6. Zusätzlicher Masquerading Router zwischen externem FW und internem Netz (Verbindungen nur von innen nach außen, auch wenn externer FW unsicher, Schutz vor Angriffen von diesem).
7. KEINE Client Isolation (falls jemand fragt), da Mitarbeiter auch Daten vom PC aufs Smartphone und umgekehrt austauschen können sollen, und bei Gästen, ist es egal.

3 Konfigurationsvorschlag