Quindi per riassumere tutto questo bel discorso ho pensato a queste piccole linee guida per migliorare la vita di tutti noi

0. AGGIORNARE TUTTI I SOFTWARE, FIRMWARE DAPPERTUTTO SEMPRE ALMENO SETTIMANALMENTE

1. pianificare la rete e stabilirne grosso modo i confini
2. Divide et impera: spezzare al massimo le sottoreti a seconda della tipologia di utenza della rete stessa. Per tipologia di utenza mi riferisco a macchine "pure" e a vari gradi di "impurita'". Valutare l'opportunita' di avere i dispositivi in una unica sottorete (diversa)
3. Tenere le sottoreti scollegate a livello 3 (routing) e possibilmente anche a livello2 (VLAN taggate diverse su cavi e porte switch diverse NON trunked)
4. Cercare di identificare sempre il proprietario di un IP in un dato momento (e' comunque richiesto dalle AUP GARR): registrazione di hardware ethernet sul DHCP che assegna IP fissi, consegna di credenziali personali solo dopo registrazione di un documento, log del firewall/NAT o del DHCP che indicano i cambi di IP (se il DHCP non assegna IP fissi)
5. Dare accessi diversi alle diverse tipologie: solo i dipendenti possono accedere alla intranet, gli altri se vogliono ci accedono tramite VPN. Trattare le reti "non pure" come estranei, come si tratterebbe la 0.0.0.0
6. Collegare al centro-stella possibilmente solo i firewall/nat delle varie sottoreti senza creare ambienti misti in cui un apparato serve piu' sottoreti (solo il centro-stella li serve tutti)
7. politiche di rete: antispoofing
8. politiche di rete in entrata: filtraggio di tutto esclusi i server
9. politiche di rete in uscita: permit in uscita solo per ESTABLISHED filtraggio in uscita su fw locali installati sull'host
10. politiche di rete in uscita: limitare l'uso della banda a NTP, SNMP DNS, SMTP
11. Posta elettronica: autenticare in SSL la posta in entrata e in uscita.
    Non permettere a nessuno l'utilizzo di SMTP senza autenticazione (a parte account di servizio delle macchine di servizio che spediscono per esempio i loro logwatch). Filtrare la porta SMTP (25) in uscita e droppare tutto escluso l'MTA di istituto.
    Smettere di fare da relay per tutti.
    Utilizzare antivirus e antispam, al preferibilmente SENZA nessuna lista RBL
12. macchine server: aggiornare e disabilitare le feature bacate non aggiornabili
13. macchine client: creare ambienti ristrertti per applicazioni criticamente vulnerabili quali browser, plugini, lettori PDF: sandbox e chroot.
    Eliminare tutti i servizi (sui server si eliminano tutti i servizi inutili, qua eliminiamo tutti i servizi!)
    limitare al massimo i privilegi degli utenti standard
    modificare nome e password degli utenti amministratori
14. Dispositivi: eliminare servizi e protocolli inutili
    Filtrare e droppare tale traffico in uscita
15. Politica di "buona pawwsord": lunga (minimo 15 caratteri), larga (che preveda minuscole maiuscole numeri e segni di interpunzione)
    dura (che duri poco, massimo 60 giorni poi va cambiata)
16. formazione del personale abilitato all'utilizzo della rete su politica delle password, phishing, rischi di sicurezza e furto di identita' etc etc

17. Prevedere dei test periodici sulla rete: scanning, penetration testing
    scarr
18. Fate uso dei servizi GARR! GINS, SCARR, segnalazioni
17. tenere il personale che si occupa di sicurezza sempre aggiornato
    leggere i siti di advisory, gli alert del GARR-CERT

e si chiude il cerchio ripartendo dal punto 0