Hårdare säkerhet i Exchange Online

1. Autentisering & åtkomstkontroller

- Stäng av legacy protocols: Inaktivera POP, IMAP, SMTP AUTH, MAPI och EWS där de inte absolut behövs.
- Conditional Access (CA): Kräva MFA vid riskabla inloggningar, blockera vissa länder/IP, kräva compliant device.
- MFA-hygien: Byt från SMS/push till FIDO2-hårdvarunycklar eller Microsoft Authenticator med number matching.
- Session control: Blockera gamla tokens och tvinga regelbunden reautentisering.

2. Skydd mot kontokapning

- Slå på smart lockout vid bruteforce.
- Aktivera Defender for Office 365 (om licens finns).
- Audit logging: kontrollera regelbundet inbox-rules och forwarding.
- Skapa alerts i Security & Compliance Center för misstänkta aktiviteter.

3. E-postflöde & spoofing

- SPF/DKIM/DMARC: använd striktare inställningar (SPF -all, DKIM på alla domäner, DMARC reject/quarantine).
- Aktivera anti-spoof policies.
- Blockera external forwarding som standard.

4. Användarhärdning

- Utbilda användare mot phishing & MFA-fatigue.
- Begränsa delegation av Send As / Full Access.
- Isolera admin-konton: ingen e-postlicens, stark MFA, dedikerad break glass-admin.

5. Övervakning & respons

- Koppla loggar till SIEM (t.ex. Sentinel).
- Hunt efter masslogins, okända inbox-rules, onormal mailvolym.
- Ha en färdig incident playbook för kapade konton.

Sammanfattning

Microsoft pratar gärna om att 'MFA är lösningen', men i verkligheten behöver man:
1. Stänga gamla protokoll.
2. Hårdare CA-regler.
3. Strikt SPF/DKIM/DMARC.
4. Proaktiv övervakning.
5. Utbildning och incidentberedskap.