Tra le minacce più comuni alle quali un'azienda potrebbe essere esposta troviamo:

1. Phishing:
    - Phishing via e-mail/sms: attacchi che cercano di ingannare gli utenti a fornire informazioni personali o sensibili, come password o numeri di carta di credito.
    - Phishing tramite siti web: siti web contraffatti che imitano quelli legittimi per raccogliere informazioni personali.
2. Malware: (ce ne sono di molti tipi, tra i più comuni abbiamo)
    - Virus: programmi dannosi che infettano i computer e possono danneggiare i dati.
    - Trojan: software dannoso mascherato da applicazione legittima.
    - Ransomware: blocca l'accesso ai dati e richiede un riscatto per ripristinare l'accesso.
    - Spyware: software che raccoglie segretamente informazioni sugli utenti.
3. Furto di dati:
    - Furto fisico di dispositivi: dispositivi come laptop o telefoni possono essere rubati, mettendo a rischio i dati aziendali.
    - Accesso non autorizzato: dipendenti o terze parti potrebbero accedere ai dati senza autorizzazione.
    - Breach dei dati: violazioni dei sistemi che portano al furto di dati.
4. Attacchi DDoS (Distributed Denial of Service):
    - Un gran numero di dispositivi invia richieste simultanee a un server per sovraccaricarlo, rendendo i servizi inaccessibili.
5. Iniezione di codice:
    - Attacchi come SQL injection o cross-site scripting (XSS) possono compromettere la sicurezza delle applicazioni web.
6. Social Engineering:
    - Attacchi che sfruttano la manipolazione psicologica degli utenti per ottenere informazioni riservate o accesso a sistemi.
7. Spear Phishing:
    - Phishing mirato contro specifici individui o aziende, spesso basato su informazioni personali raccolte in precedenza.
8. Insider Threats:
    - Minacce provenienti da dipendenti o ex dipendenti che hanno accesso privilegiato ai sistemi aziendali.
9. Zero-Day Exploits:
    - Vulnerabilità sfruttate da attaccanti prima che il fornitore del software abbia rilasciato una correzione.

10. Man-in-the-Middle Attacks:
    - Attacchi in cui un attaccante intercetta e modifica la comunicazione tra due parti legittime.
11. Pharming:
    - Redirezionamento del traffico web verso siti web contraffatti per rubare informazioni.
12. Attacchi a dispositivi IoT:
    - Attacchi contro dispositivi Internet of Things (IoT) non sicuri per ottenere accesso ai sistemi aziendali.
13. Attacchi basati su password:
    - Brute force, attacchi a dizionario, cracking di password o attacchi di guessing per ottenere l'accesso a sistemi o account.
14. Attacchi di spoofing:
    - Utilizzo di indirizzi IP o siti web falsi per ingannare gli utenti.
15. Attacchi al firmware:
    - Modifica del firmware dei dispositivi per ottenere accesso non autorizzato.

Per proteggersi da queste minacce, le aziende dovrebbero adottare misure di sicurezza robuste, compreso l'aggiornamento regolare dei software, l'implementazione di politiche di sicurezza, l'addestramento dei dipendenti e la monitoraggio costante dei sistemi per rilevare attività sospette.