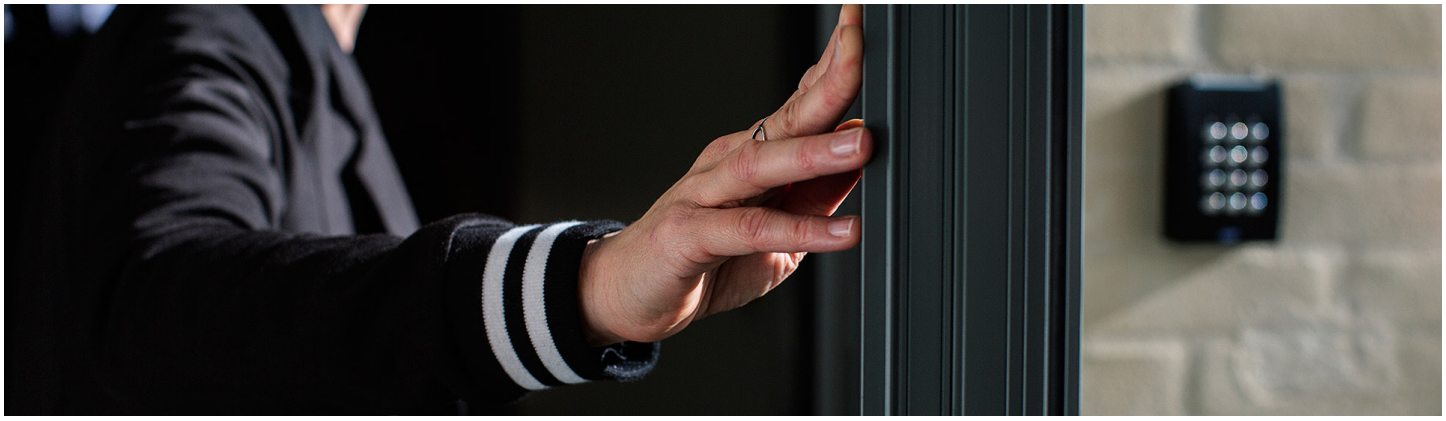

Protect your organization when receiving guests

Good advice for security before, during and after receiving foreign guests

Cooperating with foreign partners is a natural part of the work at many organizations. Knowledge sharing and networking in connection with delegation visits may be of great value. However, there is also the risk that guests will steal sensitive information to take back to their own organizations or install malware on your systems.

A step towards protecting your organization against the unauthorized transfer of knowledge is to lay down fixed procedures for handling guests. You may consider the following:

Before the visit

1. Consider the risks

Consider possible risks in connection with the visit and set up countermeasures.

2. Limit access to information and physical areas

Determine what information may be shared and, in particular, what may not. Decide on an area which the visit should be limited to and do not leave sensitive information freely accessible in the guest area.

3. Appoint employees to supervise guests

Appoint employees whose primary task it will be to supervise the visit.

4. Check who will be participating

Be aware of changes to the delegation just before the visit is to take place. Be particularly aware of embassy staff suddenly appearing on the guest list, as intelligence officers may be working under cover as diplomats. You should also be aware of guests from foreign authorities and others who stand out from the original delegation.

5. Set up IT logging
Set up IT logging to clarify whether there has been unauthorized access to your systems in connection with the visit.

6. Consider whether electronic devices should be allowed
Consider whether guests should be allowed to bring phones, tablets, cameras, smartwatches, electronic key rings etc. Such devices can be used for recording sound and images and to register GPS positions without your knowledge, or they can be used for installing malware on your systems.

7. Carry out background checks
Carry out a background check of new partners in order to determine whether there is any cause for concern. Such checks might include the owners of a company, notices concerning sanctions etc.

During the visit

1. Set up clear boundaries
Start by explaining the framework for the visit to your guests to make it clear to them what they are/are not allowed to do.

2. Use guest lanyards
Supply the guests with a guest lanyard or some other clear indication that this is a guest.

3. Supervision of the guests
Do not leave the guests unattended with any of your organization's electronic equipment such as PCs, printers, routers and servers. Be aware of guests who leave the delegation or "get lost".

4. Do not allow the installation of software or hardware
Do not allow guests to install software or hardware on your systems. This also applies to USBs with presentations. If possible, use a stand-alone computer for presentations.

5. Be aware of unexpected questions
Be alert to questions that fall outside the scope of the visit. It might be questions relating to security, sensitive political topics or the names of individuals.

After the visit

1. Go through your IT log
You should go through your IT log in order to uncover any unauthorized access to your organization's systems.

2. Be aware of subsequent contacts
Be aware of whether employees are subsequently contacted by delegation members. Does the contact give rise to any concern? Also be aware of partners wanting a repeat visit.

3. Evaluate the visit
Evaluate the visit and take action if you suspect that a security breach or some other suspicious incident may have taken place. For example, did one of the guests display suspicious behaviour during the visit? Mention your suspicion to your security officer or your immediate manager. If you assess that the incident may be related to espionage or terrorism, you should also request a confidential meeting with PET on *pet@politi.dk* ■

Further information

For more information about espionage, see the Assessment of the Espionage Threat to Denmark on *www.pet.dk*

Would you like to know more about security in connection with delegation visits? Book a briefing from PET's advisers through *raadgivning@pet.dk*