Stay secure during the summer

We give you 5 tips on how to keep security work going during the summer!

1. Have a security training course

Criminals do not only exploit technological flaws, but often rely on human weaknesses to access sensitive data. Before summer, it can therefore be a good idea to offer security training tailored to your business and the risks you face. Also make sure to have an open climate during the training so that there is room for questions, perhaps specifically questions concerning the summer months and what routines that will apply during the summer.

2. Create a clear checklist for incidents

Review incident management checklists and procedures, so there is never any doubt about how to handle an incident when, and if, it happens. This of course applies to regular staff as well as to summer staff. To be able to find ambiguities and gaps in your incident management, it is always good to have exercises where this is tested!

3. Have an incident exercise

To test and anchor your routines and policies, it is a good idea to organise an incident exercise before the summer, in which everyone including the summer staff participates. By creating a scenario where an incident occurs, any deficiencies can be detected and corrected. The least you should do is go through routines and checklists, but ideally you should simulate an incident and let the staff carry out the practical steps.

4. Review your staff's access

It is a good time to review staff access before the holiday season. It is always important to ensure that the right people have the authorisation required for their tasks, but also no more than they need. Take the opportunity to conduct a review of the user accounts that exist. If there are unused user accounts, they should be removed as they can be exploited by attackers.

5. Review your remote access

During the summer, some employees might work remotely, for example from their summer cottage. This is why it is important to review your system for remote access before summer. Remote access can be made secure by using RDP and protecting sensitive systems with an explicit security solution. Read more about Advenica's solution **here**!

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED