DCAF Geneva Centre for Security Sector Governance

DCAF'S WORK ON CERT DEVELOPMENT

Rationale

As part of its 'Enhancing Cybersecurity Governance in the Western Balkans' project, DCAF supports the development of governmental and national Computer Emergency Response Teams (CERTs). Discussions about CERT development usually centre on technical needs, such as hardware and software, or costly staff training. It is impossible to identify the most appropriate tools, however, without developing the strengths of the team to help it to better absorb new knowledge and adapt equipment to its needs.

DCAF works with CERTs in the Western Balkans to help them develop their institutional capacities. In a targeted intervention with the team, we assist them in better targeting their limited resources to do the best they can for their constituency. This involves working on identifying the team's strengths, addressing its weaknesses, and working towards a better use of the capacities of all its staff members. DCAF's support focuses on procedures as well as on people, because the work of each CERT is also supported and constrained by laws and regulations, political priorities, and institutional cultures. Being aware of this framework allows DCAF to help the CERT set realistic goals. Thanks to our extensive knowledge of public administration in Western Balkan countries, we are familiar with the wider context in which national and governmental CERTs operate. We are also aware of the level of flexibility that CERTs have in shaping their institutional structure and staff development.

Intervention phases

An assessment report forms the core of DCAF's work on the CERT's institutional development. In several reflection sessions, the team considers objectives and gaps then develops an action plan for overcoming procedural and practical challenges. Experts on CERT development and network security support the process by offering their experience of setting up and managing CERTs and of relevant tools and equipment. DCAF brings specific knowledge of the political and administrative context in Western Balkan countries to the picture.

The intervention begins with a **guided self-assessment**. The aim is to encourage the CERT to consider how to use human resources more effectively and improve the capacities of existing staff. Before the activity begins, DCAF establishes an atmosphere of confidence and trust between the experts and the CERT; to assess capacities accurately, CERT staff must feel able to speak openly and honestly. During the workshop, DCAF and the experts guide the CERT through a set of self-assessment questions adapted to the team's context. Trainers usually begin by considering which part of the CERT's mandate the team can, and should, focus on.

Many CERT teams have an overly broad mandate; as a result, staff can feel overwhelmed by the number of tasks they are expected to cover. Identifying priorities enables the team to focus on the most important tasks and to better understand which functions and services are most relevant to their constituency.

Once the CERT has re-evaluated its objectives, the team is encouraged to **identify gaps** – such as equipment and software tools – that prevent it from achieving these objectives. The experts then share **advice on the latest tools and best practices** from other European and regional countries, with a particular focus on sustainable, cost-effective solutions, such as open-source software and affordable training opportunities.

The experts also provide **guidance on procedural and professional tools** to help the CERT to fulfil its role effectively – taking into consideration its mandate and constituency. Guidance and tools may support CERTs with the following tasks: identifying standards to use in basic procedures (such as risk assessments); setting up an awareness strategy; executing cybersecurity briefings; planning communications in case of an incident (including targeted plans for the team, the ministry, various government bodies, and citizens and private companies); setting up a national cyber incident response plan; and carrying out research and enhancing situational awareness.

During the next phase, the team and the experts propose **realistic goals and timelines** for the CERT – administrative changes, purchases, and new trainings – along with the timeline – within the next 6, 12, or 18 months. The aim is to allow the CERT to take ownership of the plan and commit to implementing it.

Outcomes

DCAF has so far assisted four national and governmental CERT teams in the Western Balkans. The first two teams that have undergone training have shown striking results. DCAF helped one governmental CERT to draft a development plan, which was used to create a new organizational structure for the team and to revise recruitment, training, and retention policies. Having participated in a DCAF-led exercise, another national CERT successfully drafted an informal internal action plan to take the CERT to new levels of maturity. The team also used the input to begin revising HR policies with the aim of eventually establishing a new organisational structure as well as new recruitment, training, and retention policies.

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva
P.O. Box 1360
CH-1211 Geneva 1
Switzerland
Tel: +41 (22) 730 94 00
Email: info@dcaf.ch

DCAF Brussels
/ EU SSG Facility
24 Avenue des Arts (boîte 8)
1000 Brussels
Belgium

DCAF Ljubljana
Gospodinjska ulica 8
1000 Ljubljana
Slovenia

DCAF Ramallah
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank, Palestine

DCAF Beirut
Gefinor Bloc C
Office 604, Ras Beirut
Lebanon

DCAF Tunis
Rue Ibn Zohr 14
1082 Tunis
Tunisia