

From our Own Experts

The Evolution of WARPs

Mehis Hakkaja

This article gives an overview of the WARP concept – Warning, Advice, and Reporting Points. WARPs are a kind of CERT – light, and therefore suitable for environments where a full blown CERT might be too costly or cumbersome. They both extend and complement the work that CERTs do. In what follows, we look at the evolution of WARPs from their origins in the UK and we examine their relationship with CERTs.

The History of CERTs and the birth of WARPs

The first CERT – Computer Emergency Response Team – was created by the US Government in response to the first Internet worm in 1988. This model, also known as CSIRTs – Computer Security Incident Response Teams, has since been replicated all over the world.

Every CERT is different and can provide a variety of services like warnings and advisories to its constituency ('constituency' is CERT jargon for the user community a CERT

serves). However, to be considered a CERT, a team must provide one or more of the incident-handling services: incident analysis, incident response on site, incident response support, or incident response co-ordination.

Most European countries have one or more CERT teams in various sectors, including government, academic, commercial and others. It is clearly a well established model for providing security services. Why should we even look further?

The simple truth is that establishing and operating a functional CERT team is not a trivial commitment. Running such a team is not cheap and coverage of constituencies is still limited if we consider the European landscape as a whole. While there are over a hundred European teams mapped out in the 'ENISA Inventory of CERT activities in Europe' (available at www.enisa.eu.int/deliverables), it is clear that only a small percentage of end users and sectors are actually covered by these teams.

To improve the situation, one of the tasks of ENISA is to promote new CERTs and similar activities in EU member states and to facilitate various forms of co-operation. It

therefore makes sense for ENISA to be on a constant lookout for concepts similar to CERTs which can augment their functionality and complement their work. One such relatively new and innovative concept is the WARP model.

What are WARPs?

WARP stands for Warning, Advice and Reporting Point. The WARP model was developed by the UK's National Infrastructure Security Co-ordination Centre (NISCC) to address a slightly different security goal than CERTs: encouraging users to learn from and apply the good practice and security information that is already available in published form and within communities and interest groups. At the risk of oversimplification, one can say that WARPs aim to reduce the number of security incidents, while CERTs primarily aim to reduce the impact of those incidents that do occur.

The difference has been summarised succinctly by the creators of the WARP concept at NISCC: "WARPs perform some of the tasks of CERTs but are not expected to provide the technical response service of most CERTs".

First-hand look at WARPs

Computer Incident and Response Handling experts of ENISA visited NISCC in London in November last year to hear first-hand about WARPs from the creators of the WARP concept. Together with NISCC, we took the opportunity to observe a real-life WARP based in Kent. The 'Secure Kent' WARP (SKWARP-UK) has been providing services for 14 Local Authority partners since 2004.

As we were advised on site, the WARP provides a service of early warnings of alerts and vulnerabilities that is specifically tailored to its community. By delivering relevant content in a language understood by the community's users, and by taking steps together to mitigate specific threats within the community, the WARP is able to show tangible benefits for its members and to establish trust.

We were told that it takes about four man-hours on an average day to review all messages from about 72 sources and to categorise, customise and disseminate them to the community through the WARP's Filtered Warnings Service. This service provides each member with all the relevant warnings from a single trusted source instead of having each individual member waste countless hours sifting through the confusing plethora of online warnings. Users

also have the option to automatically select to see only categories of warnings they consider the most important and in this way they will receive even more targeted information.

Secure Kent serves a community consisting of 14 local authorities, in which four or five

members share the workload of filtering the sources. Spreading the workload over several members helps ensure the continuity of services in irregular situations. It also further underscores the point that WARPs are truly community creations, building on the collective skills and trust of their community for their operation.



A schematic view of SKWARP, the Secure Kent WARP. (Source: NISCC)

To be a little more specific, there are three core services that together embody the WARP concept:

- **Filtered warnings** service – enables WARP members to receive only security-related information which is of interest to them and tailored to their level of technical expertise.
- **Advice brokering** service – a secure environment in which WARP members can discuss security issues and help each other.
- **Trusted sharing** service – a trusted environment to facilitate the sharing of sensitive information related to real security threats and incidents between WARP members.

The WARP concept is part of an information sharing strategy to protect the UK's Critical National Infrastructure from electronic attack. At the same time, the WARP model and even the WARP Toolbox (www.warp.gov.uk/) have been placed in the public domain, and are free of charge as long they are used for non-profit services. This means that participation is open to all – indeed sometimes all it takes is the commitment of a single person with very limited computational resources to establish and run a WARP.

One good low-cost example is the Guild WARP (GUWARP-UK) that serves the online members of the Guild of One-Name studies, a genealogy society, which one would certainly not perceive as a natural information security sharing community. Such examples illustrate how WARPs can reach small communities which CERTs cannot reach directly. In fact, WARPs are best created in such small communities, to encourage the flow of information about security issues into and within the community.

It is indeed the community aspect that is the primary selling point for the WARP concept. Most WARP members join the community by choice and, as a result, are more likely to take an active role in its success, both by contributing and acting on information. In contrast, CERTs are usually imposed on users by organisational or network boundaries, which sometimes results in less user participation.

Co-operation between WARPs, with CERTs, and internationally

There are several initiatives to enhance co-operation between WARPs and beyond. An example of this is the WARP Operator Forum

that meets quarterly and which provides an opportunity for peer networking and for assisting new WARPs along. Another one is the Annual WARP Forum that held its second meeting on 15 March 2006 in London and where ENISA co-chaired a session on 'International Developments and CERT Co-operation'. This session explored ways WARPs and CERTs can co-operate and discussed how the WARP model could be replicated outside the UK.

There is also daily co-operation outside the framework of such events. The design of the WARP concept encourages bilateral co-operation between WARPs such as content sharing. In addition, in about six months' time, UNIRAS (the UK Government CERT, part of NISCC) is planning to provide automated feeds of warnings and advisories to any UK WARP that wants to receive them. Such developments further reduce the information-gathering burden on any given WARP.

There is promise for further co-operation between WARPs and CERTs as both have a slightly different set of skills and have different relationships to their constituencies. As an example, WARPs can help CERTs with their goal of having preventive advice more widely adopted, by leveraging the close relationship that WARPs have with their communities. In the future, WARPs could even provide feedback to CERTs regarding the type of information that is useful for a particular community, as well as relaying back lessons learned within the community.

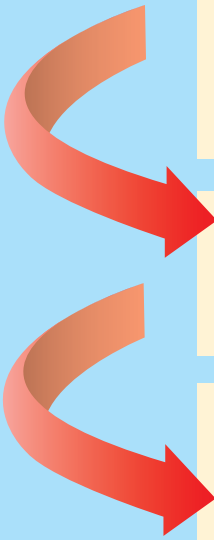
There are currently thirteen WARPs, eight operational and five developing, registered on the WARP Toolbox page (www.warp.gov.uk/WarpRegister.htm). NISCC is hoping that this number will grow to at least 20 in the UK in 2006 and that new WARPs will also emerge outside the UK.

Conclusion

The WARP concept is still evolving and we at ENISA are eager to see where this evolution leads. It certainly holds promise as an extension and complement to the CERT model and it is even hoped that the WARP model will eventually serve as a stepping stone towards the establishment of full blown new CERT teams. Indeed, while it would be good to see more CERT teams being established right away, WARPs offer an alternative approach and a more accessible first step. We encourage you to take a closer look at the WARP concept and see whether this model could serve your community's network security needs.

Mehis Hakkaja is an Expert in Computer Incident and Response Handling at ENISA

WARPs – A development model



Stage 1: Show the benefits of the WARP to the community through tailored **warning** service, so that everyone feels they are getting a personalised and valuable service.

Stage 2: Develop trust through encouraging members to help one another by sharing best practice and giving **advice** to each other through WARP facilities.

Stage 3: Encourage members to report their experiences of otherwise embarrassing attacks or problems (anonymously if necessary, through the operator) within the WARP for collective learning.

Building trust is difficult, especially virtually, which means that the third stage is not easily reached. However information sharing, even when it means revealing sensitive or potentially embarrassing incidents, can be of benefit to the entire community and can be fostered within a trusting online environment.

Such information sharing, when it can be achieved, is one of the great added values of the WARP model. In the future there is also the possibility of reports summarising shared experiences being made available to other WARPs or to CERTs that are linked to WARPs.

Once a WARP develops its skills and resources, it may wish to help its community to remedy incidents as well as to prevent them. This is the traditional role of a CERT, so it may be better to create a separate CERT to meet this demand rather than risk changing the WARP's existing relationship with its community. In this way a lightweight WARP can lead to the evolution of a full blown CERT.