The Role of Security Breach Notifications in Improving Cyber Security

Steve Purser

Attended the universities of Bristol and East Anglia where he obtained a BSc. in Chemistry and a PhD in Chemical Physics respectively. He started work in 1985 in the area of software development, subsequently progressing to project management and consultancy roles. From 1993 to 2008, he occupied the role of Information Security Manager for a number of companies in the financial sector. He joined ENISA in December 2008 as Head of the Technical Department and is currently responsible for all operational activities of ENISA. Steve is co-founder of the 'Club de Securité des Systèmes Informatiques au Luxembourg' (CLUSSIL) and is currently the ENISA representative on the ISO SC 27 working group. He frequently publishes articles in the specialised press and is the author of 'A Practical Guide to Managing Information Security' (Artech House, 2004).

Resumo

O Papel das Notificações de Violação de Segurança na Melhoria da Cibersegurança

Neste artigo analisa-se como os procedimentos de Security Breach Notification (SBN) podem ser utilizados na melhoria da cibersegurança numa envolvente transfronteiriça. A ideia central assenta no pressuposto de que dados quantitativos são necessários para melhor se compreender as ameaças envolventes, ainda que se reconheça existirem fortes condicionantes que requerem a implementação de uma recolha estruturada de dados e uma análise cautelosa de tendências.

É feita uma distinção entre SBN e Data Breach Notification (DBN). Ambos os conceitos serão relevantes para os futuros desenvolvimentos de uma política de cibersegurança da União Europeia, sendo a sua implementação requererá a adoção de requisitos específicos e economicamente viáveis em ambos os processos. Por fim, serão descritas questões relacionadas com a implementação de tais processos num contexto transfronteiriço e transcomunitário.

Abstract

This article examines how Security Breach Notification (SBN) procedures can be used to improve cyber security in a cross-border environment. The central idea is that quantitative data is necessary in order to better understand the evolving threat environment, although there are some strong limitations on this statement and it is extremely important to implement the data collection in a structured way and to analyse any trends cautiously.

A distinction is made between SBN schemes and Data Breach Notification (DBN) schemes. Both schemes are likely to play a role in future EU policy developments relating to cyber security and implementations will need to take account of the specific requirements on both processes whilst remaining economically viable. Finally, issues related to implementing such schemes in a cross-border and cross-community environment will be presented.

Introduction

Breach notification schemes provide a mechanism for institutions and enterprises to notify the competent authorities and/or the individuals affected in case of a serious security-related incident. In this article, the distinction will be made between "Security Breach Notification schemes (SBN)" and "Data Breach Notification schemes (DBN)". An example of the former scheme would be Article 13a of the EU Telecommunications Framework Directive of 2009,[1] whereas Article 4 of the ePrivacy Directive[2] provides a good example of the latter.

In the past, companies have shown themselves to be reticent in publishing data about security incidents that they have experienced. This is largely due to the fear that such publication could result in reputational damage and have a consequent impact on the success of the enterprise or organisation. For this reason, actual data characterising security incidents within the European Union (EU) has been fragmented making it more difficult to identify certain underlying trends.

The main benefit of a wide reaching breach notification scheme in the EU would be the creation of a pool of data that could be used to predict such trends across borders and across communities. Other benefits include increased opportunities to learn from mistakes and more input into improving protection mechanisms, both of which should result from the increased transparency that breach notification procedures bring about.

The possibility of introducing such a scheme across the EU Member States is an opportunity for the EU. Seizing this opportunity would enable the creation of a new source of security data, managed by a neutral third party, which could considerably increase our understanding of the nature and impact of security events throughout the union.

The Importance and Limitations of Quantitative Data

The use of past data as a tool for predicting what will happen in the future is the cornerstone of the scientific method. Such a method is however based on the

[1] Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive).

[2] Directive 2002/58/EC on privacy and electronic communications.

assumption that the data that is being collected is subject to some form of governing law or principle that can be captured and then used to predict how similar data will look in the future. Whilst experience has shown that such modelling techniques can usefully be applied to issues that are well-understood (such as proliferation of malicious code), they are in general not helpful in predicting the so-called "low-probability, high-impact events" (also called 'Black Swan events'). Unfortunately, such events tend to be extremely significant where information security is concerned.[3]

Another issue associated with the use of quantitative data is the degree of precision to which the data describes the event of interest. A virus infection could result on the one hand in nothing more serious than a ball bouncing across the screen, which is annoying but not critical, to the (stealthy) gradual destruction of data over a long period of time, which would often be catastrophic as it would infiltrate backup tapes and result in an unrecoverable situation. If the data being captured takes no account of the impact, this does not necessarily provide a lot of information on the nature of the breach.

Despite these limitations, it is clear that better data on security incidents would increase our understanding of what has happened to date and offer some degree of predictive power over how things are likely to evolve in the near future. Such data is also useful in understanding how well traditional response mechanisms coped with particular types of incidents and where such mechanisms broke down when an attack was successful. The key to getting the most out of security breach data is to understand the limitations in its predictive power and to concentrate on those trends that can be quantified and predicted.

Key Elements of Breach Notification Schemes

In the opinion of the author, breach notification schemes should provide clear descriptions of all the following points:

- Objectives and outcomes.
- Trigger conditions.
- Definition of content and data formatting rules.
- Roles and responsibilities for all actors.
- Documented procedural steps with associated timing constraints.
- Rules for handling sensitive data (including private data)

[3] An example might be *stuxnet*, which was significant because of the change of target (and hence possible impact) and represented an important change in the way in which malware was being used.

- Data lifecycle management rules.
- Adequate awareness training requirements.

Defining clear objectives and outcomes is the most fundamental requirement of a breach notification scheme, as it is these which provide the justification for defining a scheme in the first place. Furthermore, breach notification schemes should be evaluated on their ability to meet the defined objectives.

Conditions according to which breach notification procedures are triggered should be simple and unambiguous. Unfortunately, the more heterogeneous the environment to which the requirement applies, the more difficult it will be to achieve this in practice. For instance, different communities are likely to have different ideas on thresholds and how to define different severity levels.

The definition of content and suitable formatting rules is essential to ensure that the correct information is collected and that it is comparable across the contributing communities.

The need for clear roles and responsibilities, well defined procedures and timing constraints is not of course particular to breach notification, but the absence of any of these elements could result in procedures that are sub-optimal or (in extreme cases) ineffective.

Any breach notification scheme should clearly define how sensitive data (and notably private data) is to be handled. In particular, every effort should be made to ensure that the breach notification scheme cannot be itself the origin of a further breach. This kind of consideration is likely to be important where the data is provided at different levels of granularity to different audiences.

Data lifecycle management rules should clearly state under what conditions data is stored and processed, how long it is retained and when and how it will be destroyed. Backup and archiving procedures are also important in this area.

Finally, it is critical that all actors understand their role (and that of other actors) in the overall process. This will certainly require training on a regular basis and it would be prudent to include an outline o0f the requirements in this area in the definition of the scheme itself.

European Union Policy Developments

At the time of writing, European Network and Information Security Agency (ENISA) is assisting the Commission and the Member States in the implementation of two breach notification schemes.

The EU Telecommunications Framework Directive of 2009 included the addition of Article 13a, regarding security and integrity of public electronic communication networks and services. This Article states the following:

- Providers of public communication networks and services should take measures to guarantee security and integrity (i.e. availability) of their networks.
- Providers must report to competent national authorities about significant security breaches.
- National authorities should inform ENISA and authorities abroad when necessary, for example in case of incidents with impact across borders.
- National authorities should report to ENISA and the EC about the incident reports annually.

The Commission, ENISA, and the National Regulatory Authorities (NRA) have jointly proposed a single set of security measures for the European electronic communications sector and a modality for reporting security breaches in the electronic communications sector to authorities abroad, to ENISA and the EC. In May 2012 ENISA received the first set of annual reports from Member States, covering incidents that occurred in 2011. These reports covered 51 large incidents and describe services affected, number of users affected, duration, root causes, actions taken and lessons learnt.

Article 4 of the e-Privacy Directive addresses data protection and privacy related to the provision of public electronic communication networks or services. This is a Data Breach Notification article that requires providers to notify personal data breaches to the competent authority and subscribers or individuals concerned, without undue delay. The obligations for providers are:

- To take appropriate technical and organisational measures to ensure security of services;
- To notify personal data breaches to the competent national authority;
- To notify data breaches to the subscribers or individuals concerned, when the personal data breach is likely to adversely affect their privacy, and;
- To keep an inventory of personal data breaches, including the facts surrounding the breaches, the impact and the remedial actions taken.

Throughout 2011 and 2012, ENISA has been working with expert groups, national data protection authorities, industry, and the EDPS, to draft recommendations for the technical implementation of Article 4.

In general, it is likely that the EU will continue to promote breach notification schemes and it is highly likely that such schemes will be designed to be not only cross-border but cross-sector in their scope.

One of the more interesting challenges in this area is to ensure that breach notification schemes are implemented in an economically efficient manner. Thus, although SBN and DBN have different goals and are covered by different legislative instruments, it is clear that the procedures for implementing these schemes in real operational environments will have a lot in common. Implementation schemes should therefore concentrate on achieving synergies and avoid duplication of effort.

Implementation Issues

In its capacity as a centre of competence in the area of Network and Information Security (NIS), the ENISA is particularly well placed to assist the Commission and the EU Member States in the implementation of policy and legislation in this area. In particular, as any widespread breach notification scheme is likely to involve both public and private sector organisations, the implementation of such a scheme will require aligning objectives and procedures across the two communities in addition to ensuring a coherent approach in a cross-border environment. This is entirely compatible with ENISA's role of creating effective stakeholder communities to improve the level of information security across the EU.

There are however many challenges in implementing breach notification schemes in such a cross-border, cross-community environment. These include, but are not limited to:

- Difficulties in collecting and comparing data from different sources.
- Cross-border and cross community effects.
- Agreeing suitable thresholds.
- Preventing the identification of individual entities through data aggregation and anonymisation – inference techniques.
- Data protection and privacy issues.
- Problem of scalability in security – orders of magnitude.

The issue of collecting and comparing data is easy to understand – if incident data is to be collected from a variety of different environments, it is likely that the syntax and semantics will be different from environment to environment It is therefore essential to define and implement standards that allow data to from different sources to be compared.

Whereas the issue of structure is easy to understand, other cross-border and cross-community effects may be much more difficult to pin down and might manifest themselves in factors such as interpretation or significance of the data. Whilst agreeing on suitable thresholds could provide an answer to some of these concerns, it is unlikely to resolve all such issues.

If only aggregated data is to be published to a wider public, there may be a risk of employing techniques based on inference in order to link particular incidents to particular enterprises or organisations for some of the smaller Member States. Such Member States may well require more advanced data handling techniques in order to hide such relationships.

The issue of data protection and privacy is common to all Member States of course and is at the very core of the Data Breach Notification schemes. In this context, the challenge will be to define procedures for handling breach notifications that do not in themselves put personal data at risk.

Last but not least, it is clear that breach notification schemes will need to be inherently scalable if they are to stand the test of time. This is most easily illustrated by considering mergers and acquisitions, where the number of incidents that occur may grow drastically in a very short period of time.