EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TRUST SERVICES SECURITY INCIDENTS 2019

Annual Analysis Report

JULY 2020

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

CONTACT

For technical queries about this paper, please email resilience@enisa.europa.eu
For media enquires about this paper, please email press@enisa.europa.eu

AUTHORS

Aggelos Koukounas, Eleni Vytogianni, Marnix Dekker - ENISA

ACKNOWLEDGEMENTS

We are grateful for the review and input received from the experts in the ENISA Article 19 Expert Group which comprises experts from more than 30 national supervisory bodies (SBs) in EU, EFTA, EEA and EU candidate countries. The group is currently chaired by a representative of RTR Austria.

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue Number: TP-AK-20-001-EN-N
ISBN: 978-92-9204-351-3
DOI: 10.2824/047833

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Electronic trust services are a range of services around digital signatures, digital certificates, electronic seals, timestamps, etc. which are used in electronic transactions, to make them secure. eIDAS, an EU regulation, is the EU wide legal framework ensuring interoperability and security of these electronic trust services across the EU. One of the goals of eIDAS is to ensure that electronic transactions can have the same legal standing as traditional paper based transactions. eIDAS is important for the European digital market because it allows businesses and citizens to work and use services across the EU. The eIDAS regulation was adopted in July 2014 and came into force in 2016. Article 19 of eIDAS introduces *mandatory security breach notification* requirements for TSPs in the EU:

- Trust service providers notify the national supervisory body about security breaches with significant impact.
- National supervisory bodies inform each other and ENISA if there is cross-border impact.
- Every year national supervisory bodies send *annual summary reports* about the notified breaches to ENISA and the Commission.

This document, the Annual Report Trust Services Security Incidents 2019 gives an aggregated overview of these breaches, showing root causes, statistics and trends. It marks the fourth round of security incident reporting for the EU's trust services sector. The annual summary reporting for 2019 totalled 32 incident reports. A total of 27 EU countries and 2 EFTA countries take part in annual summary reporting.

The key statistics relating to the 2019 incidents are:

- **A significant increase in notified incidents:** In 2019 the notified incidents almost doubled with respect to last year, increasing by nearly 80%. This is not necessarily a sign of security getting worse. From discussions with supervisory bodies we conclude that this increase in notifications is a sign that trust service providers are becoming more familiar with the breach reporting process and their obligations.

- **System failures is the dominant root cause**: Most incidents (63%, 20 incidents) are caused by system failures. Over the last 4 years of annual incident reporting in this sector, system failures have consistently been the most common root cause of reported incidents. Typically, these cases are hardware failures and software bugs. Human errors account for almost 30% of incidents reported in 2019 while only 9% of incidents were flagged as malicious actions.

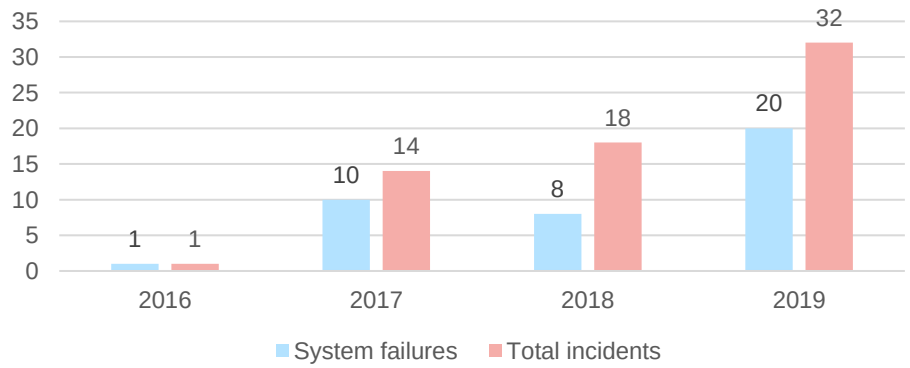
2019 ANNUAL REPORT

The number of notified incidents almost doubled.

System failures account for more than half of the incidents

System failures have been the dominant root cause in the last 4 years of incident reporting.

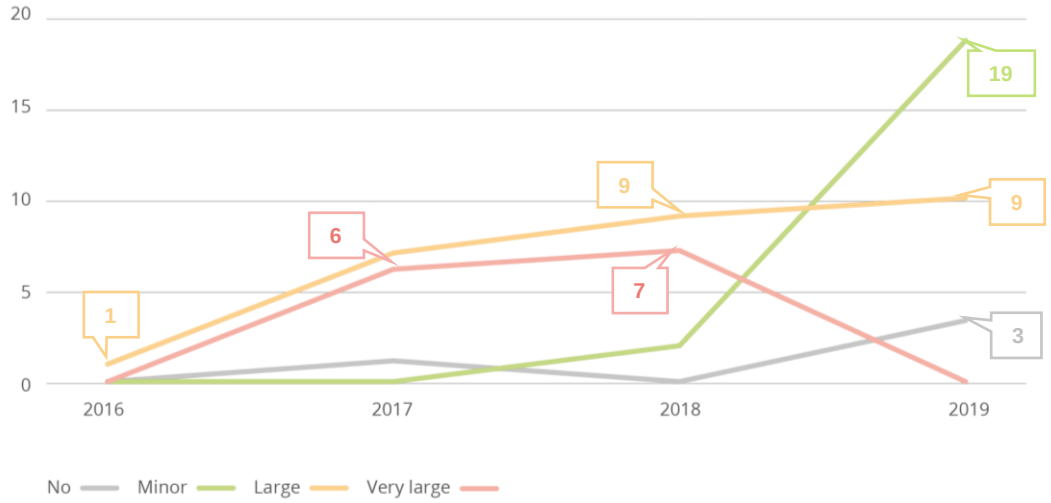
Figure 1: Total reported incidents vs system failures



- **Most reported incidents concerned qualified trust services**: More than three quarters of total incidents (78%) had an impact on qualified trust services. In general, non-qualified trust services are widely used. However in the set of all reported incidents, only a small number of security breaches concerns a non-qualified trust service (20%, 13 incidents). In most cases (80%, 52 incidents) the notification is done by a TSP also offering qualified services, reporting an incident which has affected both their qualified and non-qualified services

- **Most of the incidents were minor. Almost a third had large impact:** 31% of incidents reported in 2019 were rated as having large impact. In contrast to the two previous years, there was no incident with "very large" (disastrous) impact. We also observe a significant increase of the "minor" incidents. This is another indication that the incident reporting mechanism has become more familiar to the providers; they are reporting more incident regardless of their severity.

Figure 2: Severity of impact Trust services incidents in the EU - reported over 2016-2019



This year ENISA publishes statistics about trust services security incidents in an online visual tool. This tool allows for custom analysis of trends and patterns[1].

https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

ENISA will continue to support the national supervisory bodies with implementing the breach reporting under Article 19 of eIDAS and to work towards making this process efficient and effective, yielding useful data, for the supervising bodies, for the authorities of other sectors, as well as for the trust service providers and the organisations relying on these trust services.

Based on the experience of 4 years of eIDAS security incident reporting, the Article 19 group has provided advice and input to the Commission review of the eIDAS regulation (ongoing in 2020).

[1] See https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

1. INTRODUCTION

According to Article 19 of the eIDAS Regulation[2], Electronic Trust Service Providers (TSPs) in the EU have to notify the national supervisory bodies in their country about security incidents. Annually the supervisory bodies send summaries of these incident reports to ENISA. Subsequently, ENISA publishes an aggregated overview of these security incidents. This document gives an aggregate overview of the security incident reports submitted by the supervisory bodies over 2019.

This annual report marks the fourth round of security incident reporting in the EU's trust services sector, covering the security incidents of 2019. This document is structured as follows: In section 2 we briefly summarize the policy context, the underlying eIDAS reporting framework and we give an idea about the type of incidents reported; we mention some specific but anonymised examples. In Section 3, we dive into the reported incidents, by presenting the root cause categories, the detailed causes and the affected services. In section 4 we look at multiannual trends over the years 2016-2019. In Section 5, we draw some conclusions and make some observations.

This document only contains aggregated and anonymized information about incidents and does not include details about individual countries or individual trust service providers. Detailed discussions about the reported security incidents take place in the ENISA Article 19 expert group, which is an informal group of experts from national supervisory bodies focusing on the practical implementation of Article 19. The group is currently chaired by a representative from RTR, the Austrian regulatory authority. ENISA acts as the secretariat and supports the group with analysis, drafting, logistics, etc.

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, can be consulted at https://eur-lex.europa.eu/eli/reg/2014/910/oj

2. INCIDENT REPORTING FRAMEWORK

Article 19 of eIDAS requires trust service providers in the EU to 1) assess risks 2) take appropriate security measures to mitigate security breaches, and 3) notify/report security incidents/breaches.

eIDAS Article 19 requires trust service providers in the EU to:

1) Assess risks

2) Take appropriate security measures to mitigate security breaches,

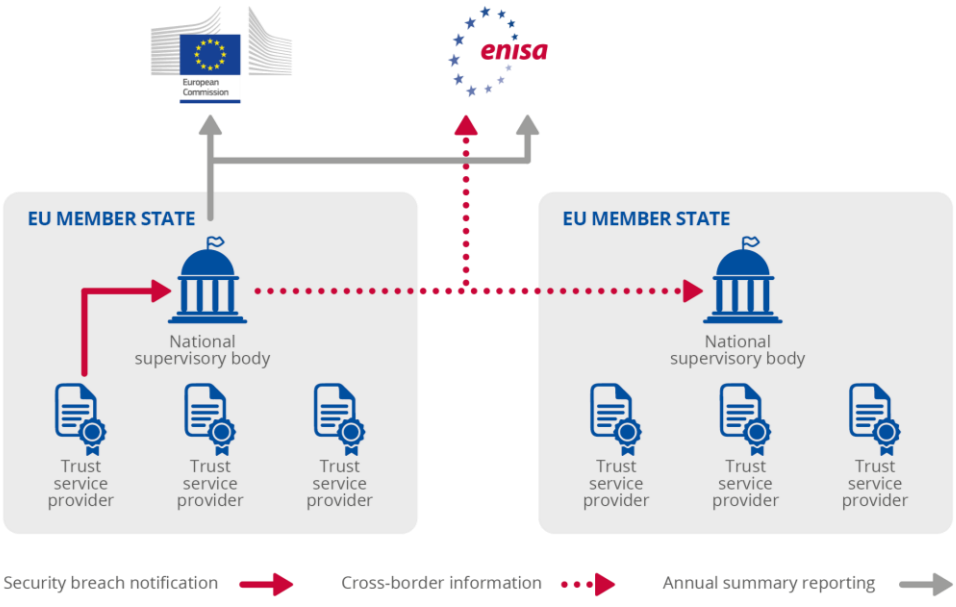
3) Notify breaches to the national supervisory bodies.

2.1 OVERVIEW OF INCIDENT REPORTING PROCESS

The mandatory security breach notification process has 3 steps:

- Trust service providers notify the national supervisory body about security breaches with significant impact.
- National supervisory bodies inform each other and ENISA if there is cross-border impact.
- National supervisory bodies send *annual summary reports* about the notified breaches to ENISA and the Commission.

Figure 3: Incident Reporting Framework for Trust Services



2.2 EXAMPLES OF SECURITY INCIDENTS

We give some anonymized examples of incidents to give an idea of the kind of incidents notified to the national supervisory bodies this year:

- [**Service affected: eSignature – generation, Detailed cause: Software bug**]: Vulnerability in the software of the fingerprint sensor of some well-known mobile devices. The secure elements of the device did not meet the security requirements as a second authentication factor for creating remote signatures. For this reason, the affected secure elements was temporarily excluded as a second authentication factor until there was a software update which fixed the problem.

- [**Service affected: eSignature – generation, Detailed cause: Faulty software change/update**]: Certificate templates have been misconfigured. The QC statement "qualified certificate" is missing from the profile. Electronic signatures created with these certificates are not qualified signatures. Thousands of certificates were generated with this profile defect over a period of more than a year. The users concerned are in several EU countries.

- [**Service affected: eSignature – generation, Detailed cause: Policy/procedure flaw]:** Certificate issued to a wrong name because a registration officer didn't comply with TSP's procedures. The certificate was revoked when the mistake was discovered.

- [**Service affected**: **eSignature, eTimestamp**, **Detailed cause: Theft or loss of equipment**]: The TSP was the victim of theft of equipment. Laptops used by main site system administrators were stolen. A report was made on the spot and a notification to the insurer was sent. The credentials were all revoked and no admins account was used before the revocation. Additional training on physical security has been implemented for staff.

- [**Service affected: eSignature, eSeal, webCertificate, Detailed cause: software bug**]: Abnormal behaviour of services, during connection to the Database. Monitoring systems detected a general slowdown accessing CA services. The anomaly was immediately detected by internal monitoring and rescheduling activities started. As a result of overloading of requests, there were problems related to accessing the DB which caused delays and timeouts. In the indicated time slot, the user could not access the CA services, while it obtained occasional timeout during authentication.

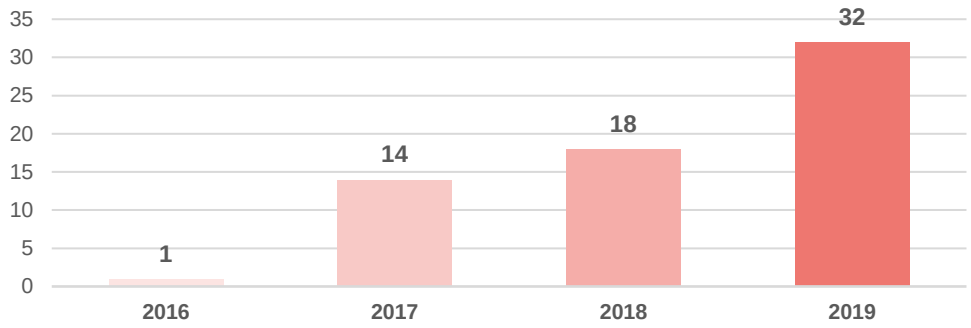
3. INCIDENT ANALYSIS

The 2019 annual summary reporting, by the 27 EU Member States and 2 EFTA countries participating in this process, included in total 32 security incidents[3]. This is the fourth round of annual summary reporting, because eIDAS came into force only recently, on the 1st of July 2016.

80%

is the increase of reported incidents compared to the previous year.

Figure 4: Trust Services Reported incidents

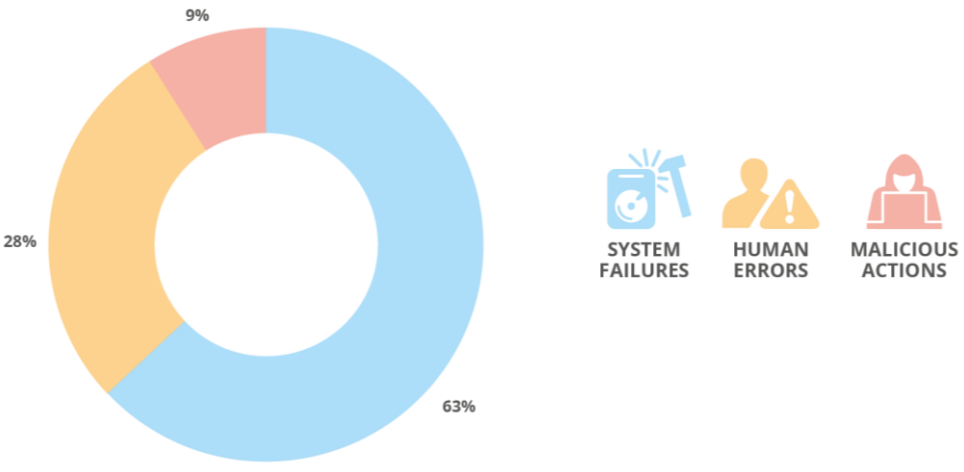


We observe an increase of nearly 80% in terms of reported incidents compared to the previous year**.** We expect the number of notified security breaches to continue to increase as the trust services market continues to grow and providers become more familiar with the breach reporting process.

3.1 ROOT CAUSE CATEGORIES

According to data received by member states, system failures are the dominant root cause accounting for nearly two thirds of total incidents reported (63%, 20 incidents). Typically, these cases are hardware failures and software bugs. Almost 30% of incidents were categorised as human errors and a minor 9% of total incidents were flagged as malicious actions. There was no incident due to natural phenomena.

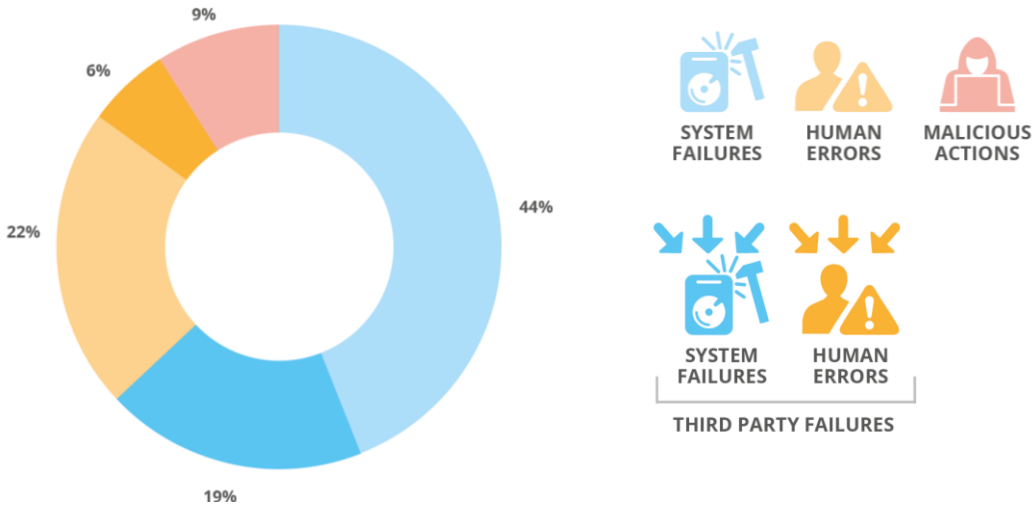
Figure 5: Root causes of TSP security incidents - 2019



[3] Note that three of the reported incidents were indicated as incidents with no impact but included in the analysis

The above graph depicts the distribution of the incidents according to their root cause. There are four main (4) categories of root causes: systems failures, human errors, malicious actions and natural phenomena. In some cases the root cause of the incidents have been reported to be also related to third-party failure. The latter is an additional cause category which can only be selected in combination with one of the above root causes. In total over 2019, 25% of incidents were flagged as third-party failures related. The division, is shown in the chart below.

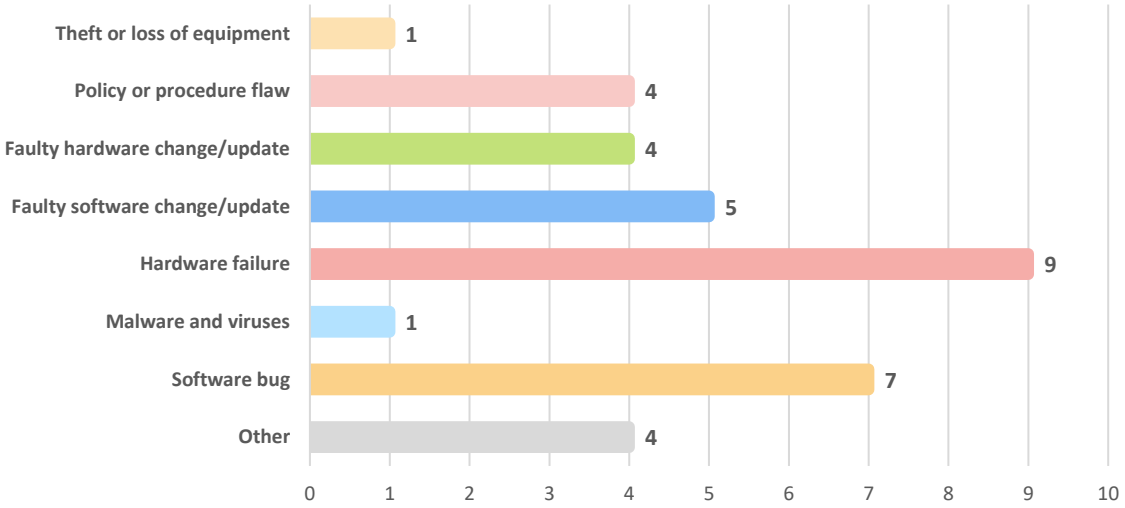
Figure 6: Root causes vs. third party failures – 2019



3.2 DETAILED CAUSES

The three most common causes of incidents are hardware failures, software bugs and faulty software change/update. Note that an incident is often not only triggered by one cause but can involve multiple detailed causes, a chain of events. This explains why the total number in the chart here add up to more than 32 which is the number of reported incidents for 2019.

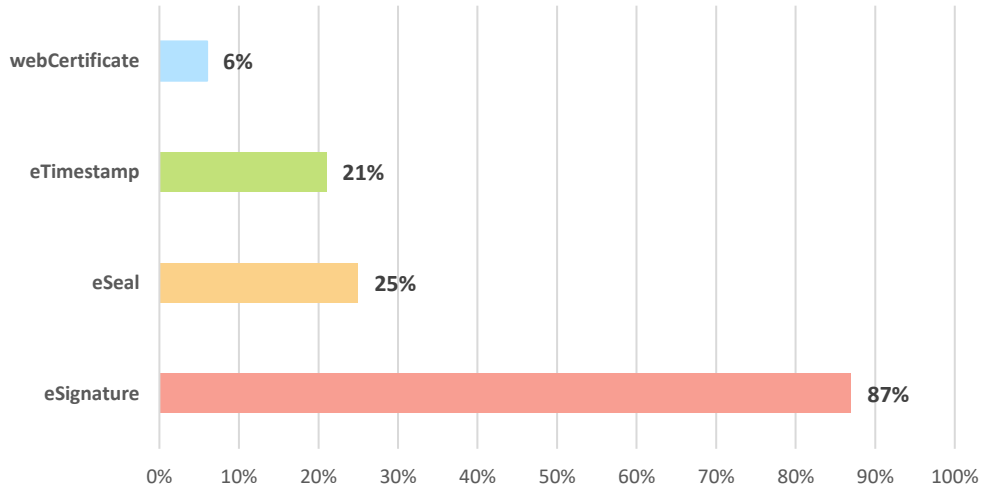
Figure 7: Detailed causes of trust services security incidents - 2019



3.3 TYPES OF TRUST SERVICES AFFECTED

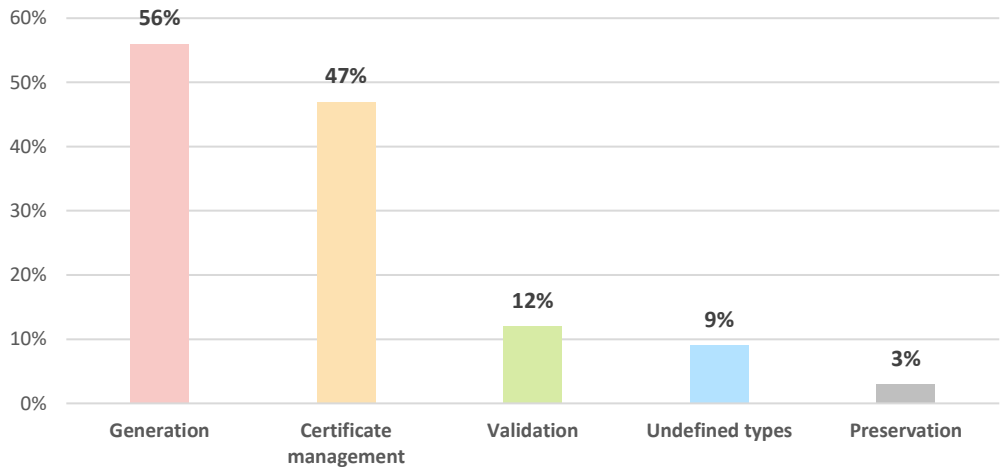
Most of the reported incidents (87%) had impact on electronic signatures. Electronic seals and timestamps were affected by one fourth (25%) and one fifth (21%) of the incidents respectively. Overall, 83% of the reported incidents in the last four years had affected electronic signature services. Both with electronic seals (29%) and timestamps services (20%) remained at the top three services affected over the years of reporting.

Figure 8: Impact of the incidents



Below we show the impact of the incidents on the subservices. The services related to the generation of signatures/seals/timestamps (56%) and certificate management (47%) are the most affected subservices.

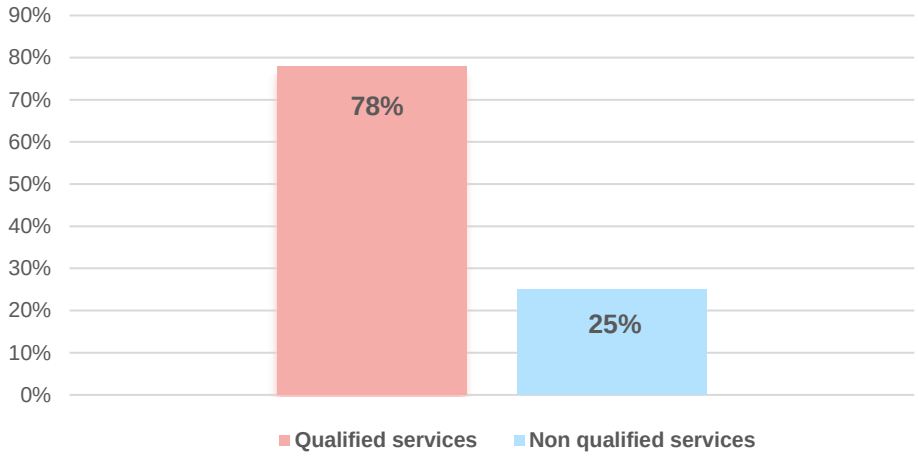
Figure 9: Impact of incidents on subservices



3.4 QUALIFIED SERVICES VERSUS NON-QUALIFIED SERVICES

This year, approximately three quarters of total incidents (78%) had an impact on qualified services (i.e. qualified signature certificate creation, qualified seal certificate creation, etc.). The corresponding percentage for non-qualified services is almost a quarter. Note that one incident report could involve multiple trust services, which explains why the percentages in the charts here add up to more than 100%.

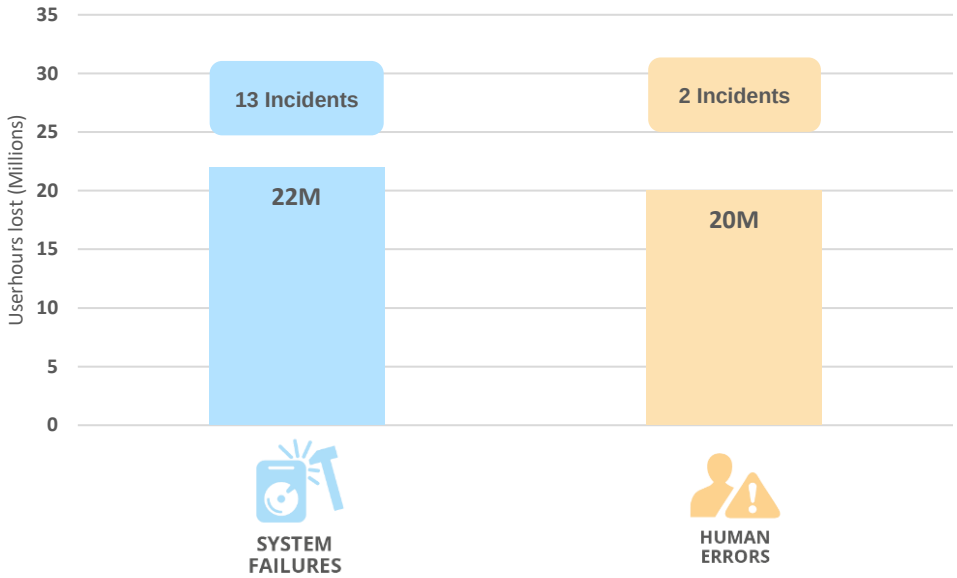
Figure 10: Reported Incidents affecting services (Qualified vs Non-qualified)



3.5 NUMBER OF INCIDENTS (OUTAGES) AND USER HOURS

Below we focus on the incidents with impact on the availability of the services (outages) and we look at the user hours lost[4]. Interestingly only a few human errors (2 incidents) account for almost the half of the lost users hours (48%, 20 M user hours). The other half is caused by system failures (13 incidents, 52%, 22 M user hours).

Figure 11: Total user-hours lost vs root cause



[4] User hours is a metric used to quantify the impact of an incident; it is the product of the number of users affected with the duration of the incident in hours. For example, 1M User Hours means 1M users were affected for one hour, or 2M users for half an hour, etc

4. MULTI-ANNUAL TRENDS 2016-2019

ENISA has been collecting and aggregating incident reports since 2016. In this section, we look at multiannual trends over the last 4 years, covering the period from 2016 to 2019. This dataset contains 65 reported incidents in total.

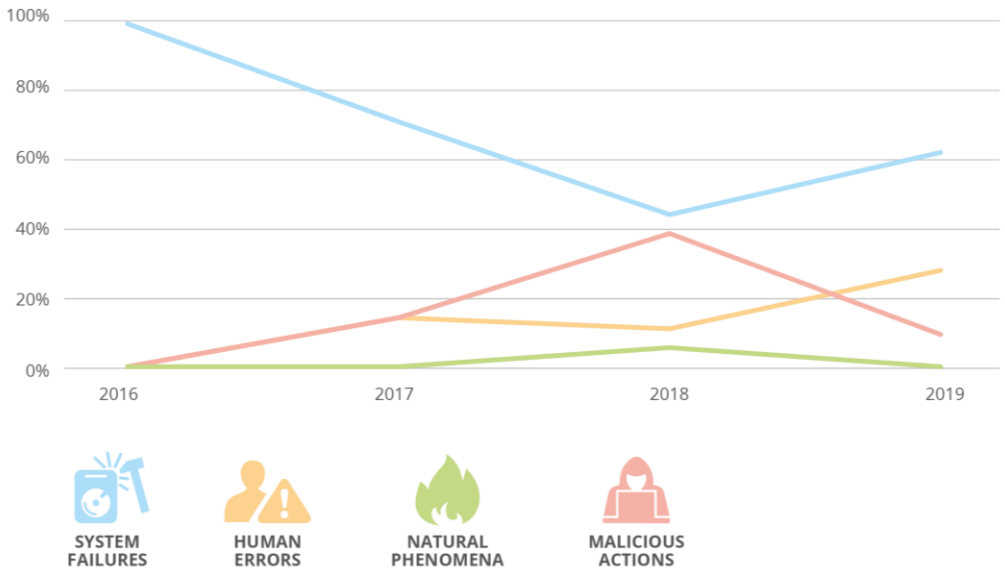
60%

of incidents are due to system failures. The most common causes were hardware failures (35%) and software bugs (33%)

4.1 MULTI-ANNUAL TREND ROOT CAUSE CATEGORIES

Over the 4 years of trust services security incident reporting, the most common root cause is system failures (60%). For this root cause, the most common causes were hardware failures (35%) and software bugs (33%). This is also the trend in the electronic communication services[5] where system failures account for almost two thirds (67%) of total incidents (722 out of 1093 incidents).

Figure 12: Root cause categories Trust services incidents in the EU - reported over 2016-2019



Around a fifth of the reported incidents (18%) were due to malicious actions and another fifth were flagged as human errors. Natural phenomena is not a common root cause in this sector. This sector operates differently than the telecom one. With large-scale aboveground infrastructure for the mobile networks, the telecom sector is more vulnerable to natural phenomena.

4.2 MULTI-ANNUAL TREND SEVERITY OF IMPACT

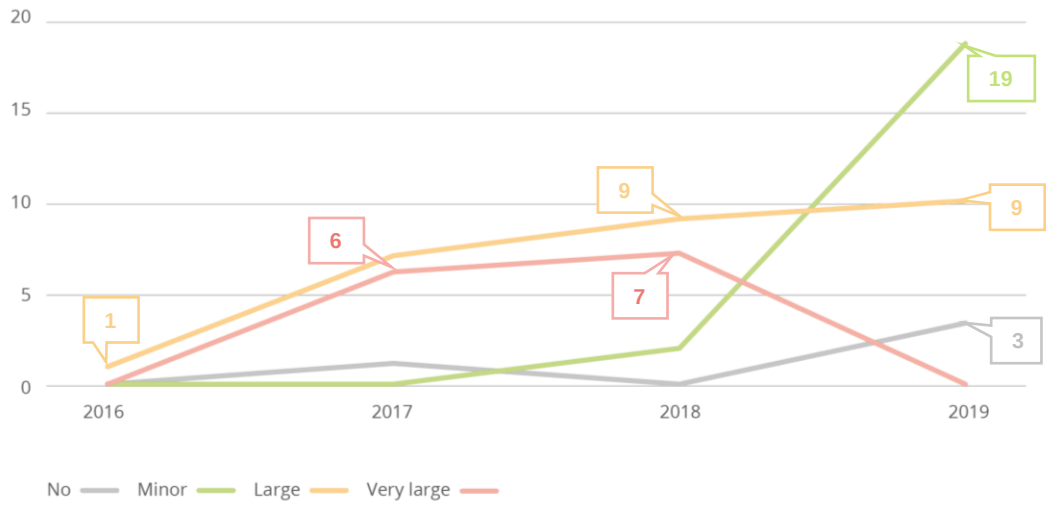
We compare the statistics for severity with the previous rounds of reporting. We follow the EU Cybersecurity incident taxonomy where the severity of the impact has the following values: no impact, minor, large and very large impact[6].

The number of incidents with large impact is almost stable the last three years. It is interesting to see that there was a significant increase of the “minor” incidents last year. This is an

[5] See ENISA Annual Report Telecom Security Incidents 2019
[6] CG Publication 04/2018 - Cybersecurity incident taxonomy

indication that the incident reporting mechanism has become more familiar and effective; providers are reporting more incident regardless of their severity. In contrast to the previous year, there was no very large (disastrous) incident during 2019.

Figure 13: Severity of impact Trust services incidents in the EU - reported over 2016-2019



5. CONCLUSIONS

5.1 KEY TAKEWAYS

The key takeaways from the 2019 incidents are:

- **A significant increase of notified incidents:** In 2019 there is a raise of nearly 80% in terms of reported incidents compared to the previous year**.** This was actually expected and is attributed to the increased adoption of trust services market and growing familiarity with this breach reporting process.

- **System failures is the dominant root cause**: Most incidents (63%, 20 incidents) are caused by system failures. Looking back at the 4 years of annual incident reporting in this sector, we observe that every year, system failures are the most common root cause of reported incidents. Typically, these cases are hardware failures and software bugs. Human errors have been the cause for almost 30% of incidents reported in 2019 while a minor 9% of total incidents were flagged as malicious actions.

- **Most reported incidents concerned qualified trust services**: More than three quarters of total incidents (78%) had an impact on qualified services while the corresponding percentage for non-qualified services is almost a quarter.

- **Most of the incidents were minor. Almost a third had large impact:** 31% of incidents reported in 2019 were rated as having large impact. In contrast to the two previous years, there was no incident with “very large” (disastrous) impact. We also observe a significant increase of the “minor” incidents. This is another indication that the incident reporting mechanism has become more familiar to the providers; they are reporting more incident regardless of their severity.

5.2 OBSERVATIONS

Beyond the numbers in the incident reports, we make two general observations below about the overall process, based on our experience with eIDAS incident reporting and discussions in the Article 19 group:

- **Supervision of, and incident reporting by, non-qualified services:** Non-qualified trust services are widely used. A good example is website (TLS) certificates, which are a staple of online/internet security. Globally around 80% of websites use web certificates. LetsEncrypt alone had issued a billion website certificates in February 2020.

  There have been scores of major security incidents with web certificates, also in Europe. Take for example, the Diginotar incident[7] of 2011 (Certificate authority hacked, fake certificates for google.com), which led to a major disruption of Dutch e-government and eavesdropping of Iranian citizens, or, more recently, the DNSpionage[8] attacks of 2018-2019, in which DNS poisoning and fake certificates were used to eavesdrop on public and private sector organizations in the EU.

  However, in the set of reported incidents, only a small number of security breaches affect a non-qualified trust service (20%, 13 incidents). In most cases (80%, 52

[7] https://threatpost.com/what-you-need-know-about-diginotar-hack-090211/75611/
[8] https://www.wired.com/story/sea-turtle-dns-hijacking/

incidents) the notification is done by a TSP also offering qualified services, reporting an incident which has affected both their qualified and non-qualified services.

This suggests there is under-reporting of security breaches with non-qualified trust services. It is good to mention here that under eIDAS, non-qualified services are subject to ex-post supervision. This means that only after a security breach, the supervisory can take action and assess the security of the trust services. This explains that supervisory bodies are not always aware of, or in contact with, the trust service providers and their services. When an incident happens, the supervisory body often learns about it in media reports, and does not get informed about incidents directly.

- **Reporting about vulnerabilities and attacks-in-the-wild:** There is a clear need to exchange information not only about actual incidents with impact at a TSP's trust service, but also about attacks and vulnerabilities. Since the ROCA case happened, information sharing between supervisory bodies has improved. There were more recent examples of such cases, like the Minerva attack[9] and the attacks bypassing the signature validation in pdf[10]. These cases highlight, once more, the need for raising awareness and exchange information with a broad group of entities, i.e. research communities, CSIRTs, national supervisory bodies, owners of potentially affected eID schemes, etc. Good information exchange and communication between competent authorities enables timely assessment of the situation and makes it easier to respond and prevent or mitigate incidents.

  ENISA facilitates the information sharing between national authorities by providing the technical means to the supervisory bodies for sharing this kind of information. We are also adapting and extending the CIRAS incident reporting tool to better support this kind of cross-border communication better. We are currently piloting with the owners of the national eID schemes, who need to notify incidents under article 10 of the eIDAS. And there are other types of incidents which are noteworthy and interesting to exchange information about, like near-misses, or incidents prevent by activation of security measures like revocation of devices or certificates.

The eIDAS Regulation and the eIDAS incident reporting have been in place for more than 4 years now. We have been improving the incident reporting process, together with the Article 19 group. This year, under eIDAS Article 49, the European Commission is reviewing the eIDAS Regulation itself, in order to report to the European parliament and to the Council. This eIDAS review is an opportunity to address some of the above-mentioned issues and gaps. We look forward to supporting the Commission and the EU Member States with implementing eIDAS security incident reporting in an efficient and effective manner.

[9] https://minerva.crocs.fi.muni.cz/
[10] https://www.nds.ruhr-uni-bochum.de/media/ei/veroeffentlichungen/2019/02/12/report.pdf

TP-AK-20-001-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-351-3
DOI: 10.2824/047833