NIS Directive Battleground insights

SECTIO AUREA®

Who?

I spent a decade working at IBM, where I contributed to some of the most sophisticated service projects in Central and Eastern Europe.

I was a solution manager to a very recognized local player in cybersecurity in Romania for more than 4 years.

I played a key role as a Global Portfolio Manager for Cybersecurity Services at Atos - Eviden, one of the leading multinationals in the field of cybersecurity, managing global cybersecurity projects in areas such as identity management and cloud security. I

Certified NIS Auditor, CISM, CISA.

I have served many clients as a consultant in the implementation of the NIS Directive in various fields (water companies, banking, utilities).

I have participated as a certified NIS auditor in various audit missions in complex or difficult environments.

Since 2018, I decided to start a mission around a concept of crowdsourcing and microservices. Pivoted several times until success was achieved.

Under **Sectio Aurea** I provide value in cybersecurity, with very mature people, in a flexible and competitive manner, with **the highest quality.**

Sectio Aurea is the latin translation from the golden section, Phi (or φ from the ancient Greek alphabet), also known as Fibonacci's number, the golden number, the divine proportion, is an essential number, present in all fields of activity (mathematics, biology, design, architecture, biology).


Why Battleground insights?

SECTIO AUREA®

Because we are in a war. Hybrid. Unseen until too late.

Russian Cyber Actors are Exploiting a Known Vulnerability with Worldwide Impact

FORT MEADE, Md. - The National Security Agency (NSA), Federal Bureau of Investigation (FBI), and co-authoring agencies warn that Russian Foreign Intelligence Service (SVR) cyber actors are exploiting a publicly known vulnerability to compromise victims globally, including in the United States and in allied countries.

The U.S. Cybersecurity & Infrastructure Security Agency (CISA), the Polish Military Counterintelligence Service (SKW), CERT Polska (CERT.PL), and the United Kingdom's National Cyber Security Centre (NCSC-UK) collaborated with NSA and the FBI to assess the SVR cyber actors' recent malicious activities.

The SVR cyber actors, who are also known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and NOBELIUM/Midnight Blizzard, have been targeting Internet-connected JetBrains TeamCity servers globally as early as September 2023. Victims identified in the report include companies that provide software for billing, medical devices, customer care, employee monitoring, financial management, marketing, sales, and video games, as well as hosting companies, tool manufacturers, small and large IT companies, and an energy trade association.

National Security Agency/Central Security Service, 13 December 2023

Since January 2022, Russian cyber actors have targeted government, academic, private sector, and critical infrastructure entities in Denmark, Latvia, Lithuania, Norway, Poland, the US, and Turkey for cyberespionage purposes, as well as entities in Finland and Sweden, both of whom applied for NATO membership following the Russian invasion of Ukraine in February.

In early April, Ukrainian authorities publicly reported several spear-phishing attempts attributed to FSB cyber actors targeting Ukrainian and unspecified EU government targets.

In late April, a previously unknown and financially motivated hacking group (Hive0117) dropped a copy of DarkWatchman malware in a phishing campaign impersonating a Russian agency and targeting Eastern European countries.

In mid-May, an unknown threat actor targeted German users interested in the Ukraine crisis by using a decoy site to lure users into downloading malicious documents, which infected them with a custom PowerShell remote access Trojan (RAT) and stole data.

We assess that Russia is almost certainly in the process of developing cyber capabilities against targets in the EU and NATO, including the US and Canada.

Canadian Center for Cybersecurity, Cybert Thread Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine 2024

SECTIO AUREA®

We are in a hybrid war

Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility.

A hacking group with ties to the Russian government is suspected of carrying out a cyberattack in January that caused a tank at a Texas water facility to overflow, experts from US cybersecurity firm Mandiant said Wednesday.

The hack in the small town of Muleshoe, in north Texas, coincided with at least two other towns in north Texas taking precautionary defensive measures after detecting suspicious cyber activity on their networks, town officials told CNN. The FBI has been investigating the hacking activity, one of the officials said.

The attack was a rare example of hackers using access to sensitive industrial equipment to disrupt regular operations at a US water facility, following a separate cyberattack last November on a Pennsylvania water plant that US officials blamed on Iran.

CNN, 17 April 2024

"Russian hackers were inside Ukrainian telecoms giant Kyivstar's system from at least May last year in a cyberattack that should serve as a "big warning" to the West, Ukraine's cyber spy chief told Reuters."

Reuters, 5 January 2024

"Since the beginning of this year, a **hacktivist group known as the Cyber Army of Russia, or sometimes Cyber Army of Russia Reborn, has taken credit on at least three occasions for hacking operations that targeted US and European water and hydroelectric utilities**."

Wired, 17 April 2024

"Germany has summoned a **top Russian envoy over a series of cyber-attacks targeting members of the governing Social Democrats and its defence and technology sector**. "Today we can say unambiguously [that] we can attribute this cyber-attack to a group called APT28, which is steered by the military intelligence service of Russia," the German foreign minister, Annalena Baerbock.

…

Germany's interior ministry said a series of cyber-attacks attributable to the Russian military intelligence service GRU had also targeted the country's logistics, defence, aerospace and IT sectors.

…

The Czech Republic said its institutions had also been targeted. "Czechia has long been targeted by the APT28."

The Guardian, 3 May 2024

Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

The NSA, FBI, CISA, Department of Health and Human Services, the Republic of Korea (ROK) National Intelligence Service, and the ROK Defense Security Agency issued a joint Cybersecurity Advisory to highlight ongoing ransomware activity against Healthcare and Public Health Sector organizations and other critical infrastructure sector entities.

America Cyber Defence Agency , 9 Ferbruary 2023


In nature, in a war
The predator always targets
The weakest from the herd

Critical Questions I had 4 years ago

Where are the weakest from the herd?

If they fall, what is the potential impact?

What is going outside the space of regulated, big or multinational companies?

How mature are the regulated?

Key Answers – Non-regulated space

Various maturity levels

NIS adoption is triggered by digitalization and risk appetite

We can be better

Key Answers –Regulated space

Habit debt.

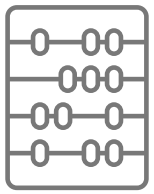
Technology debt.

Skills shortage

SECTIΦ AUREA®

Why are we here?
Key Root causes

Key Root causes



Romanian market maturity & Low Digitalization

Leadership high risk appetite

Complex & unclear regulatory framework versus low maturity.

Awareness play

Controlling?

Complex & unclear regulatory framework

Very complex rules.

Many methodological ordinances, some never executed

Redundancy

Acronyms

No detailed methodology on what an OSE must to, to show compliance

Contradictory and unclear terms for auditors

NIS auditors should have the auditing framework in detail.

Articolul 5

(1) În procesul de stabilire a impactului incidentelor se va avea în vedere următoarea scală:

Tabel I.1 – Scala impactului incidentului

Impact	Descriere	Valoare medie
SCĂZUT	II_{FE} sau II_{FD} este unul scăzut, efectul asupra furnizării serviciului nu este disruptiv, alerta procesată nu este I_{SC}, iar riscul producerii unui I_{SC} nu există.	$V(PE) < 2$
MEDIU	II_{FE} sau II_{FD} este unul mediu, efectul asupra furnizării serviciului este unul disruptiv, alerta procesată este I_{SC}, iar riscul producerii unui I_{SC} este unul limitat.	$2 \leq V(PE) < 4$
RIDICAT	II_{FE} sau II_{FD} este unul ridicat, efectul asupra furnizării serviciului este unul disruptiv semnificativ, alerta procesată este I_{SC}, iar riscul producerii unui I_{SC} este unul ridicat.	$V(PE) \geq 4$

(2) Valoarea medie a parametrilor de evaluare se stabilește pe baza următoarei formule:

$$V(PE) = \frac{\sum_{i=1}^{n} V(PEC_i)}{n}$$

unde **V(PE)** reprezintă media aritmetică a valorilor parametrilor de evaluare comparativă V_{PEC}, iar **n** reprezintă numărul parametrilor comparați.

Hotărâre de Guvern 1003 din 23/11/2020 - Normele tehnice de stabilire a impactului incidentelor pentru categoriile de operatori de servicii esenţiale şi furnizori de servicii digitale

Hotărâre de Guvern 601 din 21/06/2019 - Metodologia de stabilire a efectului perturbator semnificativ al incidentelor la nivelul reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale. [Art. 8 alin. (9)]

Complex & unclear regulatory framework

Very complex rules.

Many methodological ordinances, some never executed

Redundancy

Acronyms

No detailed methodology on what an OSE must to, to show compliance

Contradictory and unclear terms for auditors

NIS auditors should have the auditing framework in detail.

OSE - operator de servicii esențial
PEANIS - procesul de acreditare s
administrare
PEGEC - procese de gestionare a
cibernetică pentru asigurarea continu
PEIREV - proces de identificare,
informatice
PGMAVU - program pentru mana
PONIS - politica de securitate a re
PPSIA - plicul cu parole utilizate
PRADE - procedură privind mana
PRAPC - procedură pentru asigura
PRAPMA - procedură pentru asig
PRASA - program de prezentare a
PRASI - procedură privind accesul și securitatea resurselor și informațiilor
PGASP - program de asigurare a securității personalului; document prin care OSE identifică obiective și stabilește cerințe de securitate pentru fiecare etapă a relației avute de către angajați
PRECAS - procedură privind evaluarea conformității NIS și efectuarea auditului de securitate a rețelelor și sistemelor informatice
PRECDI - procedură privind etichetarea și clasificarea datelor și informațiilor
PRIMSA - procedură pentru gestionarea informațiilor primite și, după caz, a măsurilor de securitate adoptate pentru protejarea NIS
PRISA - program de instruire în domeniul securității pentru angajații care utilizează rețelele și sistemele informatice care stau la baza furnizării serviciilor esențiale
PRISAC - procedură de interconectare la serviciul de alertare și cooperare al CERT-RO
PROCIS - procedură privind organizarea gestionării crizelor în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale
PRODAIS - procedură pentru detectarea incidentelor de securitate care afectează rețelele și sistemele informatice
PROFIT - procedură privind filtrarea traficului
PROLD - procedură privind lucrul la distanță
PROMNIS - procedură pentru menținerea securității rețelelor și sistemelor informatice
PROMRE - procedură privind managementul recuperării datelor în caz de dezastre, precum și în caz de incidente severe de securitate cibernetică
PRORAI - procedură pentru gestionarea, răspunsul și analiza incidentelor care afectează funcționarea sau securitatea rețelelor și sistemelor informatice
PRORIS - procedură pentru raportarea incidentelor de securitate
PRORUVI - procedură pentru reducea riscurilor legate de utilizarea unei versiuni învechite
PROSES - procedură privind segregarea și segmentarea rețelelor și sistemelor informatice utilizate pentru furnizarea serviciilor esențiale
PROSRE - procedură de stabilire a relațiilor ecosistemului; documentul include interconexiunile (relațiile externe) între rețelele și sistemele informatice și terți
PRUSIA - procedură privind utilizarea sistemelor informatice de administrare
PRUSME - procedură privind utilizarea suporților de memorie externă
RAEC - raport de evaluare a conformității

Ordin Nr. 1.323 din 9 noiembrie 2020
pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale. Printscreen from Anex 1.

Awareness play. Where is the control

No public actions from authorities towards OSE after major security breaches

No actions towards OSE which are not in compliance with the law (NIS audit submission)

No clear response or no response to OSE how to fulfil the law

Some critical OSE does not implement NIS Law.

And they will continue not to act until first penalty.

Demotivates OSEs who are doing the minimal.

because for them penalties triggered NIS adoption.

SECTIO AUREA®

Looking forward.

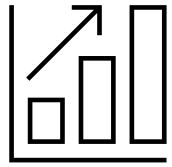
Looking forward

Simplification of regulatory framework.

- Simplify system and method to show compliance
- Simplify auditing framework and guidelines

Follow up

- Digitize the NIS Compliance reporting
- Follow up on law execution for OSEs
- Monitor Auditors work.



Continue awareness

SECTIΦ AUREA®

Madalin Bratu CISA CISM

Director General

+4 0722 154 062

madalin.bratu@phi.ro

www.phi.ro