HealthManagement.org

LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES

VOLUME 22 • ISSUE 6 • € 22

ISSN = 1377-7629

Cybersecurity: Preventing the Worst-Case Scenario

THE JOURNAL 2022

Cybersecurity: Preventing the Worst-Case Scenario

Vito Petrarolo | Chief Digital Officer and Digital and Privacy Office Manager | Health and Social Care Agency of Apulia (AReSS) | Project Manager | Telemedicine Operations Center for Chronic Conditions and Clinical Networks (COReHealth) | Apulia Region | Italy
Giovanni Maglio | Lawyer | AReSS Digital Transformation System Executive | Lead Auditor | ISO/IEC 27001/2013 | Italy

Cyber threats and vulnerabilities cannot be completely eliminated as no informatic system is completely impenetrable. However, certain measures can be implemented to limit the likelihood of a breach or reduce its scale and consequences. Effective leaders must focus on building mission-critical systems with the goal of quickly recovering from both anticipated and unexpected attack scenarios. Elements of the whole system must be integrated and coordinated to prevent the worst-case scenario.

Key Points

- The increasing digitalisation and systems interconnection in healthcare has left more exposed to and impacted by cybersecurity attacks.
- Cybersecurity must become an integral part of patient safety and should be considered an enabler for ensuring the resilience and availability of key healthcare services.
- The issue of cybersecurity is becoming a pervasive bullet on the agendas of healthcare companies and public administrations.
- Cybersecurity and personal data protection should not be the result of complying with a legal obligation but a cultural process to be implemented and continuously adapted to the changing reality.

The unstoppable increasing digitalisation and systems interconnection in the healthcare sector has left more exposed to and impacted by cybersecurity attacks. Healthcare is an already targeted sector, and we can expect more to arrive in years to come. The high propensity to pay a ransom, the value of patient records and often inadequate security are the main issues that attract cybercriminals.

Cybersecurity is crucial for patient safety, but it has often been underestimated. This requires that cybersecurity becomes an integral part of patient safety through changes in human behaviour, technology and processes as part of a holistic solution, and it should be considered as an enabler for ensuring the resilience and availability of key healthcare services.

It must not be forgotten that healthcare is a complex system in which multiple, heterogeneous and dynamic factors interact, including the plurality of healthcare services, specialised skills and professional, technical and economic-administrative roles, and the heterogeneity of processes and results to be achieved.

The ongoing drive to integrate systems, especially in the health sector (interoperability), makes the boundaries of the systems themselves ever wider and more exposed, often involving those structures of organisations that, while not directly handling health data, represent entry points for attacks on the entire system and thus also on sensitive data.

As if this were not enough, the COVID-19 pandemic pushed the health sector to the limit and further highlighted the importance of protecting health services and medical data (personal and non-personal), both from a cybersecurity and data protection perspective.

According to Cost of a Data Breach Report 2022 issued by IBM Security, healthcare sector breach costs hit a new record high, with the average breach increased by nearly USD 1 million (about €953.000) to reach USD 10.10 million (about € 9.530.000). This new target has let the healthcare breach costs the most expensive industry for 12 years in a row,

increasing by 41.6% since the 2020 report, followed by financial, averaging USD 5.97 million (about €5.700.000), pharmaceuticals at USD 5.01 million (about €4.780.000), technology at USD 4.97 million (about €4.737.000) and energy at USD 4.72 million (about €4.500.000).

In 2020, the World Economic Forum issued the Global Risks Report, where cyberattacks on critical infrastructure were rated the fifth top risk in the same year, becoming the new normal across sectors, among which, of course, healthcare stands in pole position. Such attacks have affected entire cities, and public and private sectors alike are at risk of being held hostage by organised cybercrime entities which are joining forces, even because their likelihood of detection and prosecution is estimated to be as low as 0.05% in the United States (Eoyang et al. 2018).

Thus, the issue of cybersecurity is becoming a pervasive bullet on the agendas of healthcare companies and public administrations, in view of the fact that they are considered critical infrastructures by almost all governments, and even due to the large spikes in malware in 2021: healthcare (121%) and government (94%), as SonicWall stated in its 2022 Cyber Threat Report.

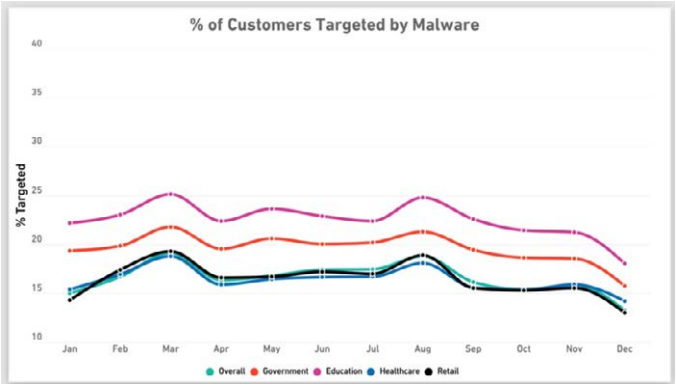

Figure 1: Customers targeted by malware. Source: SonicWall 2022 Cyber threat report

Furthermore, the recent regulatory changes in the European Union, including the NIS (Network and Information Security) Directive (EU) 2016/1148, the European Regulation 2019/881 (the so-called Cybersecurity Act), the General Data Protection Regulation 2016/679 (EU) known as GDPR, and the so-called NIS2, just approved by the European Parliament, are part of this trend where cybersecurity is an integral part of Europeans' security, as clearly affirmed in the EU's Cybersecurity Strategy for the Digital Decade issued at the end of 2020.

From an Italian perspective, the legal framework is quite composite and spans from the transposition of the European Directive to several internal regulatory acts, including the one establishing the National Cybersecurity Agency (ACN) and the one imposing the implementation of the National Framework on Cybersecurity for Public Administration, based on NIST Cybersecurity Framework. These regulatory standards are valuable tools, as well as unmissable opportunities to facilitate change.

At this stage, while a lot of professionals strive for additional governmental regulation to ensure patients and their data are protected, many healthcare leaders understand that voluntary compliance with the strictest standards is the only way to avoid further and, sometimes, onerous compliance regulations.

In this context, AReSS (Regional Strategic Health and Social Agency of the Apulia Region), which is part of the wider regional healthcare system, has decided to set its security posture according to this principle because cybersecurity and personal data protection should not be the result of complying a legal obligation, but a cultural process to be implemented and continuously adapted to the changing reality.

From the point of view of IT security, the Apulia Region, located in the south of Italy, in which the organisation AReSS is based, uses the cloud service provider Innovapuglia, an in-house company with 100% public participation. Innovapuglia deals with all aspects relating to the security of information systems, from the network to the cloud.

AReSS is entrusted with the internal management of security. AReSS has pinpointed four pillars on which it has established its security posture for a healthcare sector organisation:

- Increasing visibility
- Improving third-party security
- Raising staff awareness of cyber threats
- Complying with regulation

Security risks cannot be thwarted if they are not known. An attack surface monitoring solution immediately visualises all vulnerabilities associated with cloud solutions within a private network.

The Agency, via an external provider, has created an infrastructural and security audit and assessment service aimed at identifying the priority and necessary interventions to be implemented to raise the level of security and improve the performance of the infrastructure. This assessment involves:

- Listing the risks perceived by the customer and defining the main safety objectives;
- Verification of the existence and possible evaluation of a risk analysis required by EU; Regulation 2016/679 and related hypothesised countermeasures;
- Verification of the implementation of the AgID (Italian Digital Agency) minimum measures;
- Verification of the suitability of authentication mechanisms;
- Verification of the backup execution methods to evaluate their exposure to malware attacks;
- Verification of the current perimeter or similar security measures;
- Verification of tools to prevent virus/malware infections;
- Check coverage of necessary measures referring to provisions of a general nature of the Data Protection Authority (e.g. regulation about system administrators);
- Threat Intelligence services.

In 2014, IBM reported that 17% of breaches in the critical infrastructure industries were due to supply chain attacks

Figure 2: Enisa 2022 threat landscape for supply chain attacks

where a third-party business partner was the attack vector, while in 2020, the revelation of SolarWinds already hinted at the potential of supply chain attacks to attackers (and defenders). In recent days, the European Union Agency for Cybersecurity (ENISA) mapping emerging supply chain attacks found 66% of attacks focus on the supplier's code.

These data say that a lot of data breaches occur via a compromised third-party provider. In other words, if incident response efforts only focus on internal cyber threats, the security teams have merely addressed less than half of the risks that facilitate breaches.

Improving the security posture of all third-party vendors requires an orchestrated effort between risk assessments, security assessments and vendor tiering. To this extent, AReSS has set a procedure where the procurement office should check that third parties provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the general security level will meet the requirements set by regulation. As a result, the security and risk management team partners with other offices to prioritise and manage risks to digital supply chains.

Furthermore, the Agency has planned and organised specific training courses for both the personnel involved in data processing and those who do not process the data because these are part of the Agency's security chain. In fact, they can represent potential entry points into the network and, therefore, into computers, and from there, who knows where else.

According to the 2014 IBM Cyber Security Intelligence Index Report, human error was a major contributing cause in 95% of all breaches, usually not directly, but providing access to cybercriminals against their will. More recently, in the 2022 Data Breach Investigations Report by Verizon, the human element continues to drive breaches, involving 82% of breaches; whether it is the use of stolen credentials, phishing, misuse, or simply an error, people continue to play a very large role in incidents and breaches alike. The World Economic Forum's Global Risks Report 2022, cited above, also confirms these estimates: 43% of breaches come from homegrown threats, and 95% of cybersecurity alerts are attributable to human error.

Investment in staff training in public healthcare administration is a key principle by which the principles of digitisation and dematerialisation, but above all, the security of processed data, can be developed. The effectiveness of an organisation's processes is directly related to how consistent its staff is in following these processes and policies. To this end, organisations should provide comprehensive training on IT security measures and the risks involved if staff members do not comply with these procedures.

For example, AReSS staff is trained to recognise a suspicious email and not to open anything (attachment or embedded link) that could be potentially dangerous. They are also instructed to inform IT if they have any doubts about the authenticity of an email message, even by referring to free cybersecurity resources available online.

At AReSS, we think it's important to develop the ability to recognise that the threat is real; indeed, while it is easy to see how someone with malicious intentions might target a bank or a retail shop to illegally access tangible physical assets, it is often more difficult to see why and how someone might breach the systems of a healthcare organisation. In addition to the periodic training of staff, the Agency, under the guidance of the Chief Digital Officer, has published a series of thematic manuals, including one about cybersecurity and another about personal data protection.

However, the growing concerns about the security of personal

data and health IT systems have led to the copious current legislation, trying to regulate in an attempt to create an organic and homogeneous protection system, even though full regulatory compliance is not easy to pursue due to high fragmentation of the legal framework.

Last but not the least, AReSS was partner in an Horizon 2020 European Research Project, named Threat-Arrest (www.threat-arrest.eu), which developed an advanced training platform incorporating emulation, simulation, serious gaming and visualisation capabilities to adequately prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk cyber systems and organisations to counter advanced, known and new cyber-attacks in three different sectors: maritime, energy and healthcare. AReSS was the pilot for healthcare systems and the staff was trained with this online platform.

Conclusion

Obviously, threats and vulnerabilities cannot be completely eliminated, so reducing security risks is particularly challenging. While no informatic system is completely impenetrable, there are certain measures that organisations can implement to help limit the likelihood of a breach or at least reduce its scale and consequences. Today's organisation can never hope to entirely avoid security failure, and effective leaders focus on the organisational resilience of mission-critical systems with the goal of quickly recovering from both anticipated and unexpected attack scenarios. All the elements of the whole system must be integrated and coordinated to prevent the worst-case scenario since it is precisely between the folds of such dynamism and heterogeneity that threats and dangers to security may be concealed, aiming for a zero-trust security approach.

Conflict of Interest

None. ■

REFERENCES

Eoyang M, Peters A, Mehta I, Gaskew B (2018) To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors. Third Way.

HealthManagement.org

Promoting Management and Leadership