REGULATORY UPDATES

THESEUS REGULATORY UPDATES ON PATCHING

EU Developments

Cyber Defence Policy: The EU Commission recently presented their Cyber Defence Policy, which highlights the importance of a robust cybersecurity framework for the defence community. The Commission will draft non-binding recommendations for a high common level of cybersecurity, and re-states the importance of CSIRTs in swiftly informing the defence community of vulnerabilities and available patches. The policy will also pay special attention to the cybersecurity of critical infrastructure and be assessed annually by means of Commission reports. Source: here and here

ENISA Top Cyberthreats for 2030: ENISA has published an infographic on the top cybersecurity threats likely to emerge by 2030. Holding a strong position in the top 3 is the exploitation of legacy systems within cyber-physical ecosystems, reflecting the recent importance placed on patching regulation. Other primary risks are those of a supply-chain compromise of software dependencies (n1) and cross-border ICT service providers as a single point of failure (n9), both of which are heavily linked to supply-chain vulnerability management. Source: here

Cyber Resilience Act (CRA) feedback period extended: The feedback period for the CRA has been extended to **12 January 2023**. The proposal so far has been largely well received, with organisations such as Eurosmart welcoming the proposal and its increased cybersecurity requirements. The organisation does call for EU-harmonized minimum standards and further clarification on the standardisation approach. Source: here and here

EDPS Opinion on CRA: The European Data Protection Supervisor has shared their opinion on the CRA proposal. The EDPS largely welcomes the proposal, particularly commending the similar fines to the GDPR and the importance played on security by design in annex 1. The EDPS does call for privacy by design to be included in the essential product requirements, and highlights a need for specification of the synergies and hierarchy with other EU laws. Source here

(*This submission was made available by Ben Kokx, from stakeholder Philips)*

HIGHLIGHTS

EDPS OPINION CRA

The EDPS requests additional provisions on harmonization of CRA with other legislation

US UPS CYBERSECURITY

The US has introduced numerous minimum cybersecurity standards for critical sectors

GLOBAL BREACHES UP 70%

Global data breaches were up by 70% in the third quarter of 2022

US Developments

Detailed Cybersecurity Standards imposed for Railway: The TSA has presented a new directive raising the minimum standards of cybersecurity care for railroad operators. The new standards impose new fines and enforcement options, and bolsters the TSA's ability to assign liability to companies that are accused of failing to meet the minimum standards. Meeting or exceeding the standards is therefore incentivised, as it will create a strong litigation defence. This directive is part of a series of US efforts to increase cybersecurity, swiftly followed by the inclusion of the chemical sector in new cybersecurity rules. A further extension of these cybersecurity standard initiatives is likely, with the newly released voluntary performance goals serving as an expected baseline. Source here, here and here

Increased Cybersecurity expectations for Medical Devices: The FBI has published a report to reiterate the high cybersecurity responsibility of medical device companies (such as Philips) to tackle unpatched vulnerabilities, due to the risks they pose to patient safety and healthcare facilities' functioning. Special attention was paid to the underlying software lifecycles, as many legacy devices are still in use yet have stopped receiving manufacturer support for patches. The FBI recommends increased endpoint protection and access, asset and vulnerability management. Source here

FTC takes action against CEO of delivery app for security failures: The FTC has proposed an order which binds the CEO of an alcohol delivery app to specific data security requirements for failing to take action when alerted to security problems 2 years prior to a breach. The action is likely to be the start of a push by agencies to hold individuals in leadership roles accountability for an organisation's cybersecurity failures. Source here

No Cyber Insurance coverage for state-sponsored attacks: The case against the US-based insurance company Zurich has been settled outside of Court. The insurance company refused to cover damages under its cyber insurance that were the result of state-sponsored cyber-attacks. The case already led to other cyber insurance companies to release cyberwar exclusion clauses. Source here and here

Global Developments

Global data breaches up by 70%: The IAPP has shared a report by SurfShark which reveals that global data breaches are up by 70% in the third-quarter of 2022. A total of 108.9 million accounts were breached, most of which were in Russia. Some countries saw an over 1000% increase in breach rates. Source here and here

Apple commits to only patching latest OS: Apple has updated their 'software updates' page to reflect their committal to only fully patching the latest version of its OS. Despite providing security updates for multiple OS versions, only users of the latest version should expect to be fully protected. Whether this is in response to the new EU ARES proposal is unclear and its interplay remains to be seen. Source here

WANT TO CONTRIBUTE YOUR OWN UPDATES AND REGULATORY FINDS?

CONTACT E.M.ROOIJ@TILBURGUNIVERSITY.EDU

THESEUS PROJECT
https://project-theseus.nl/