zscaler™

WHITE PAPER

Enhancing Cybersecurity In the EU: An In-Depth Look at the NIS2 Directive and Its Impact On M&A/D

1. Overview

In response to growing cybersecurity challenges, the European Union (EU) will revitalize its cybersecurity directive NIS (Network and Information Security), the legislation framework on measures for a high common level of cybersecurity across the European Union. The updated directive is commonly known as NIS2 that member states need to transpose into national law by October 17, 2024.

The NIS framework traces its origins to the growing recognition of cybersecurity as a critical component of national and economic security within the EU. The first iteration was adopted in 2016 in response to increasing cyber threats targeting essential services and critical infrastructure operators. The NIS Directive aimed to ensure a high level of cybersecurity resilience across key sectors such as energy, transportation, finance, healthcare, and digital infrastructure. It mandated member states to identify operators of essential services (OES) within these sectors and impose cybersecurity obligations on them, including risk management, incident reporting, and cooperation with competent national authorities.

2. NIS2 – Emerging governance, risk, and compliance requirements

Building upon the foundation laid by the NIS Directive, NIS2 represents a significant evolution in EU cybersecurity policy. One of the most notable changes is the expansion of the directive's scope to include digital service providers (DSPs) alongside OES. NIS2 affects all entities that provide essential or important services in 15 industry sectors (see https://nis2directive.eu/who-are-affected-by-nis2/) and differentiates two archetypes of entities which are "Essential Entities" (EE) with a size threshold of >250 employees and annual turnover of >€50 million as well as "Important Entities" (IE) with a size threshold of >50 employees and annual turnover of >€10 million.

This expansion into new industry sectors (from 7 to 15) and service areas reflects the growing importance of cybersecurity in the modern economy and acknowledges the need to mitigate any cybersecurity risks associated with mobility, marketplaces, search engines, and cloud services. In addition to widening the scope, NIS2 introduces several new provisions to enhance cybersecurity resilience and response capabilities, including (see also https://nis2directive.eu/nis2-requirements/):

- Enhanced security requirements on both OES and DSPs in order to mandate the implementation of risk management measures, appropriate technical and organizational controls, and incident reporting mechanisms. ("To comply with the new Directive, organizations must take measures to minimize cyber risks.")
- Measures for supply chain cyber security between company and direct suppliers. ("Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers")
- More stringent penalties for non-compliance with the directive, aiming to ensure effective enforcement and incentivize organizations to prioritize cybersecurity measures in several sectors. ("NIS2 requires corporate management to oversee, approve, and be trained on the entity's cybersecurity measures and to address cyber risks.")

More Affected Sectors

NIS2 expands the number of covered sectors from 7 to a total of 15 to protect more vital areas of society.

Stricter Requirements

Compared to NIS1, NIS2 dramatically increases the requirements for enforcing cybersecurity.

Worse Repercussions

In addition to heavy fines, NIS2 non-compliance can also lead to legal ramifcation for management teams.

Sources: https://nis2directive.eu/what-is-nis2/

3. NIS2 – What are the impacts on mergers, acquisitions, and divestitures (M&A/D)?

In general, transactions bare huge risks on their own. They stress standards, are full of one-off scenarios, operational effectiveness is typically low and status quo of existing technology architecture is unclear. Specifically, transactions bare unique challenges when it comes to cyber attacks and related risks. In a recent survey conducted by Zscaler ThreatLabz, where 647 Cybersecurity Experts were interviewed, one result was that 69% of interviewed persons reported concerns around the impact of M&A on the existing VPN infrastructure spotlighting the potential vulnerability that arise from organizational changes, e.g. integration of disparate networks. 56% of organizations in the survey experienced one or more VPN-related cyberattack in the last year—up from 45% the year before—highlighting the growing frequency and sophistication of attacks targeting VPNs (see Zscaler "ThreatLabz 2024").

Technology M&A/D leaders now need even more to take over responsibility to offset the risk of legacy technology such as VPNs or firewalls with the envisaged transaction results (e.g. synergy savings). From an infrastructure perspective the following points are to consider:

Due Diligence (DD): Transacting companies need to conduct thorough pre/post closure due diligence regarding the cybersecurity posture of the entities involved. This includes higher efforts on assessing their compliance with NIS2 requirements especially with regard to some key questions, e.g.

- General cybersecurity posture; what are the attack vectors including network security posture and what is the legacy complexity incl. maintenance/governance efforts compared to the level of automation (e.g. level of AI usage).
- Risk management practices; what is the concept to monitor, understand and prioritize risks. Are mitigation actions derived from historic cases? Is prescriptive analytics used, where do the data sets come from (data synthesis conducted in-house or outsourced).

Not having quick, sufficient transparency into the technology estate bares huge risks to prolong DD process or miss impactful shortcomings in the target. A special NIS2 lens should be taken into account when reporting back red flags.

Post-Closure to Day 1: integrating or divesting technology including network and security is a complex endeavor, especially when attempting to align disparate networks,

cybersecurity frameworks, processes and leading practices on organizational level. Successful M&A/Ds consequently plan and integrate NIS2 principles on enterprise and solution architecture level early on in order to ensure value creation from the integrated system landscape.
Imperative for the NIS2 technology architecture are simplicity (lean footprint), effectiveness (support relevant e2e processes) and efficiency (automate, lean governance). Typical pitfalls that counteract NIS2 technology architecture planning are:

- Opaqueness of the acquired companies network (M&A specific)—not having enough transparency even after post closure is a common problem that prolongs evaluation timelines and dismantles holistic conceptual planning. An exhaustive overview of the technology estate is paramount to let leaders plan and execute accordingly.
- Enabling user to application connectivity already takes months to years. Additional regulation that comes on top should not extend this timeline further. New M&A/D playbooks need to adapt NIS2 while taking out factory-like activities like network integration and point solution consolidation.
- Expert knowledge becomes a rare resource once again. NIS2 experts are likely to be in high demand when it comes to future state solution architecture planning, while project timelines might get stressed depending on their availability. A well defined documentation of the as-is technology blueprint helps to provide recommendations on shortcomings fast and adapt to a NIS2 compliant state.

Day 1 to Day 2: recent Zscaler internal surveys have shown that primary ownership of NIS2 does not necessarily sit in the CIO/CISO area (42%) but also in business areas (58%). This is also the reason why successful M&A/D anticipates NIS2 requirements on a tactical level within the overall operating model (plan activities accordingly) and needs clear accountability into all relevant end-to-end business process areas.
Involved transacting parties must address cybersecurity responsibilities, incident reporting requirements, and liability allocation in contractual agreements (e.g. Migration Agreement, TSA) to mitigate legal and financial risks.

- From a governance perspective, a single point of contact in the respective entities (transacting entities and third parties) is paramount to ensure NIS2 regulative success (collaboration).
- From a technology solution standpoint, leaders should be capable of leveraging business-wide telemetry (live data) to understand and mitigate potential risks and threats early on. Not having intelligent solutions that detect and prevent potential cyber threats early on taking into account not only your internal users but also third parties, production (OT) and workloads becomes a huge hypothesis for any organizational NIS2 leader.
- Incident response capabilities of all parties involved becomes now more of a constant triangulation between the organizational entities (typically the service desks of the transacting companies), third parties and national authorities. Robust but lean processes, well defined interfaces and auditable documentation is important to ensure smooth operational transition.

- Data protection and privacy considerations drive organizations must ensure that data transfers comply with applicable legal requirements (personal data, GDPR) and that cybersecurity measures are in place to protect data integrity and confidentiality (especially intellectual property that sits in the EU).

4. How Zscaler can help solve NIS2 challenges

Zscaler fundamentally provides security and network as a Cloud service. Our three major building blocks of the platform are:

- Connecting users, applications, workloads, B2B with each other securely via a brokered connection. All organizational assets (not only users) are securely connected via the Zero Trust Exchange (ZTE).
- Running the largest inline security cloud in the world securing data at rest. At global scale, the Zscaler Cloud processes 400+ billion daily transactions while 150+ million threats are blocked.
- Turning data into knowledge and delivering insights. Equipped with predictive and prescriptive data analytics applied on the ZTE, we make use of the data that is processed daily resulting in high value insight generation.

That brings Zscaler in a unique spot when it comes to adopting NIS2 in M&A/D.

Reduce complexity: First and foremost, Zscaler offers a centralized platform for managing compliance with NIS2 and other cybersecurity regulations. In transactions, when standards are stressed and regular operation is not always possible, organizations thrive for effective solutions to secure connectivity, integrity and security while being able to have transparency and control over all of your organizational assets within or outside of your organization. This is where Zscaler shines while improving your ability to report against NIS2 requirements, streamlines efforts and reduces administrative burden.

Leverage a complete, scalable platform: Effective cybersecurity in M&A/D requires a set of services that run on a global scale in order to be an efficient measure to prevent breaches and secure your organization. It is not enough anymore to protect users and Intellectual property only. NIS2 expands cybersecurity also to external providers (B2B), sites, production OT technology but also workloads as an expression of digital value creation (especially DSPs relevant).

Zscaler Zero Trust is built and field proven to deliver against these ambitious requirements and comes on top with many tools for risk management and mitigation, ranging from business insights to live performance monitoring and monetary impacts if a risk is not getting mitigated. On top, Zscaler telemetry data (80+ out of the box) makes your as-is cybersecurity posture transparent and comprehensible (e.g. in an audit). The completeness of Zscaler networking and security capabilities, combined with a fit-for-purpose Zero Trust architecture without legacy gives you a powerful tool at hand to effectively understand risks in an M&A/D and prioritize respective actions for mitigation.

Accelerate your M&A/D and free up capacities: Zscaler has supported more than a thousand transactions, for many F2k companies, reducing timelines for network and security integration. It is obvious that in traditional M&A/D, a huge portion of activities carried out on the infrastructure side is on network/security evaluation, mitigation,

adoption and harmonization. At Zscaler, a user connects with the Zero Trust Exchange and the respective application and does not reside on the network.

Setting up the connectivity takes a fraction of time (up to 50% reduction in time to value) and resources (up to 75% reduction in operational complexity) by contrast to the traditional approach to integration. As a result of our approach to M&A/D, Zscaler contributes effectively to free up time from your key people in order to focus on additional value driving activities that need attention.

Enhance cybersecurity and reduce risk: Zscaler reduces the traditional attack surface caused by VPNs and firewalls entirely by ensuring that only authenticated and authorized users and devices can access applications and data. This method is particularly effective in preventing attacks that exploit network vulnerabilities, thereby aligning with NIS2's emphasis on risk management. Even more, through its centralized inspection and policy enforcement, Zscaler ensures that all traffic, regardless of user location, is inspected and secured before accessing corporate resources.

5. Call to action

In situations where standard operation is not feasible organizations need sophisticated instruments to stay on top of things. Successful M&A/D leaders take cyber considerations and compliance requirements like NIS2 early on into account in order to deliver against their monetary targets.

1. **Make your technology architecture NIS2 compliant:** Architecture is a foundational element to be successful against cyber attacks and become NIS2 compliant. Castle and Moat concepts bare too many attack factors (firewalls, VPNs) for hackers, especially in M&A/D situations where standards are stressed and regular operations are off limits. Zero Trust architecture approaches are not only less prone to attacks due to reduced outside–in visibility and robustness by design, but also counteracts lateral movement scenarios where bad actors can cause severe damage and reputation loss to your organizations.

2. **Remove complexity in times of change by utilizing platforms:** Platform solutions that provide security and connectivity as a service are especially strong in situations of change. While traditional solutions work well in standard operations (incl. maintenance), these may come to its limits when organizations frequently buy/sell or see change as a driver for new opportunities. Traditional technology stacks can be seen as "Jenga towers" – many point solutions that constitute a set of services. In times of change, the robustness of the "tower" is at constant risk. Here a platform remains stable and operable as a significant level of service operations is yet outsourced by definition (as a service).

3. **Instantiate replicable processes and avoid one-off scenarios:** Replicability and expectation conformity are both key in M&A/D. Successful leaders invest in solutions and playbooks that are highly repeatable in order to counteract one-off scenarios that can cause high security risks and ultimately reduce transaction value. Organizations need best practice playbooks (Infrastructure related) that help boost integration and divestment timelines (from years to days) and de-risks challenges relating to immature processes. Time-consuming exercises like post closure due diligence or user-application mapping should become automated, streamlined activities rather than manual exercises that enhance risks and non-compliance.

4. **Invest in prescriptive cybersecurity technology:** Successful leaders in security and M&A/D invest in solutions that help sustain normal operations or improve business agility, no matter the circumstances. Solutions that provide transparency throughout the organization in breadth and depth that are easy to manage are paramount to run a compliant business. Visibility combined with data analytics (historical, prescriptive data) help identify threats and mitigate them early on so that they won't harm your business. Bottom line, transparency, the right level of knowledge and the right people involved help to become and stay NIS2 compliant, even in M&A/D situations.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com