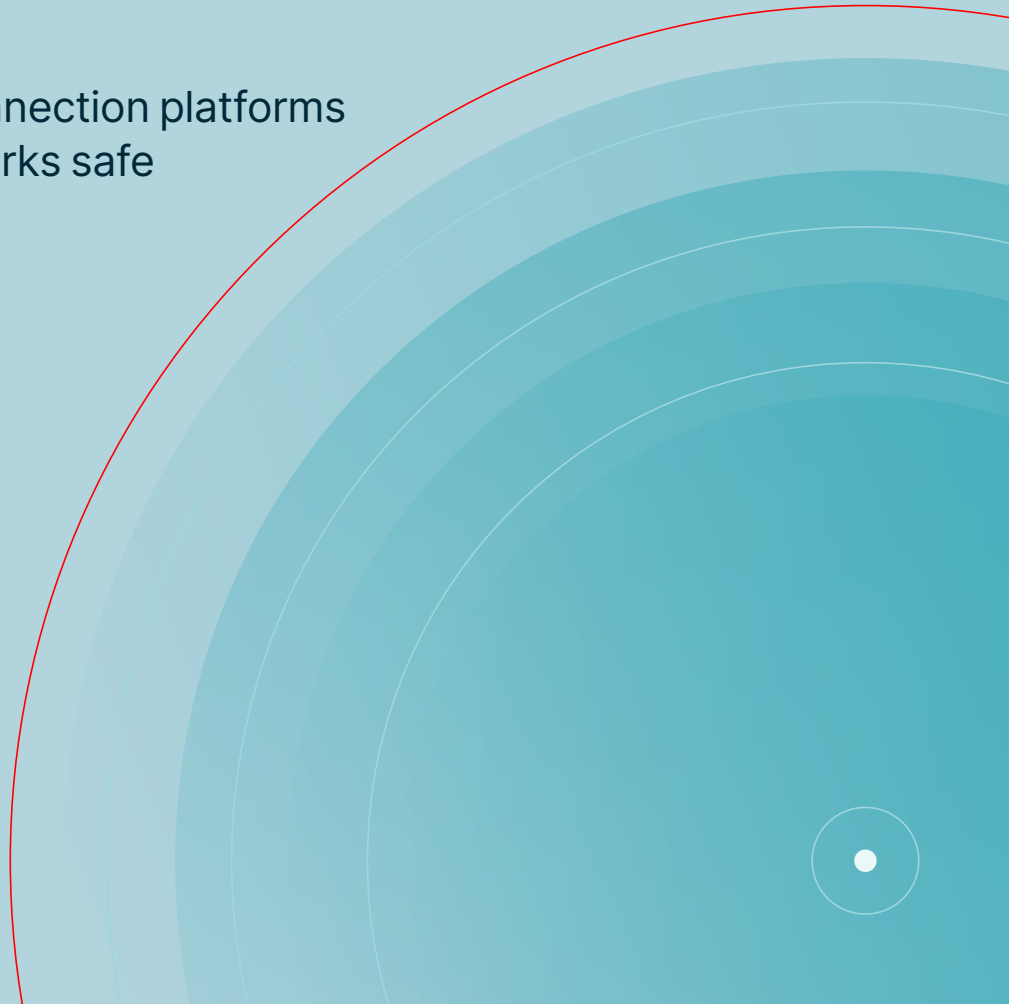
DE-CIX

WHITE PAPER

Organizational, security, and resilience measures at DE-CIX

How we keep our interconnection platforms and our customers' networks safe



PUBLISHED AUGUST 2023

Internet Exchanges (IXs) such as DE-CIX are a vital part of the Internet infrastructure. They provide a platform for networks to easily interconnect and they therefore create a rich ecosystem of networks. As the Internet is realized through the interplay of thousands of organizations and networks on a shared platform, it naturally comes with risks – threats that can massively influence the quality of data traffic, can prevent networks from sending traffic at all, or can cause the traffic to be routed to the wrong destination.

DE-CIX, as a large IX operator, implements a range of security and resilience measures to keep our interconnection platform and our customers' networks safe. In the following, we briefly summarize what kinds of protection measures we have implemented.

Security and resilience measures on different layers

DE-CIX operates specific security and resilience measures on different layers of the well-known OSI Model. Some layers have more impact than others when securing our platform, but together they build a comprehensive solution:

- The physical layer (L1) – data center and fiber optics layer
- The data link layer (L2) – peering LAN (Ethernet & MAC) layer
- The network layer (L3) – IP layer
- The transport-application layers (L4-L7) – BGP & software layer

Threat mitigation techniques

	Security		Resilience	
L1 physical layer	Data center access control Own identity & access Management system		• Core redundancy: N+1 for larger exchanges • Data center: 2 electricity supplies (1+1) • Optical fiber cable: georedundancy (1+1) • Patch robots: 2+1 redundancy • Subsea cables: 1+1 redundancy	Routers (Nokia 7750 SR-s, 7950 XRS (e), 7250 IXR series): Redundancy for air conditioning, electricity (1+1), two control planes (high availability)
L2 data link layer	Peering LAN: • EVPN-access lists (ACL) • Static MAC ACLs to avoid routing loops		MPLS path failover (1+1 redundancy)	Routers: Link access groups
L3 network layer	Route server RPKI filtering	DDoS protection: Blackholing, Blackholing Advanced	Route server redundancy	
L4-7 transport & application layer	Analytical: • Testing • Static code analysis in continuous integration process • Ad-hoc penetration test by external partners	Constructive: • Development process – git branching and pull reviews • Scrum, transparence, and agility IRR filtering	Design pattern: • Isolation • Loose coupling • Communication between components • Redundancy	Alarm and monitoring system

Overview of security and resilience mechanisms at DE-CIX

Security mechanisms

L1: We work with many data center operators who all comply with certain standards of operation. We ensure compliance with the ISO/IEC 22237 (in Europe, DIN EN 50600) standard in all locations for building, planning, and using the data centers. Since electrical systems are a big part of a data center, we further ensure compliance with, for example, DIN EN 62638 / DIN VDE 0701/0702 and IEC 60364 (in Germany DIN VDE 0100, while in particular parts 100 and 410-444 also apply). Our safety and security standards are based also on German governmental recommendations ("BSI IT Grundschutz") and we are ISO 27001 certified. The data centers in which we operate require access lists, key cards, identification, and biometric data for accessing. Some of other security mechanisms inside the data centers are surveillance cameras, alarm systems, protective grids, door and rack locks, security guard escort for the visitors and 24/7 monitoring. Also, we run our own identity and access rights management system, such that only authorized DE-CIX employees can enter the data center and obtain access to the racks.

L2: We use static ingress and egress access control lists (ACL) with MAC addresses to avoid routing loops inside the Peering LAN, and we employ a global MAC-filter for ethernet broadcast.

L3: ACL-based filtering is used for dropping and shaping traffic, e.g., in the case of DDoS attacks or other unwanted traffic. On the DE-CIX route servers we provide a high level of routing security. For this purpose, Resource Public Key Infrastructure (RPKI) validation is used.

L4-7: To help our customers mitigate the effects of Distributed Denial of Service (DDoS) attacks against their networks, we offer customer-triggered Blackholing. Blackholing allows a network operator to signal a blackhole by using the BGP BLACKHOLE community. As a result, all the traffic flowing to the victim will instead be dropped on the DE-CIX platform, so that the victim's resources are protected against the increased loads caused by the attack. The blackholed traffic will never reach the customer's access.

Standard Blackholing removes unwanted traffic completely from the customer's port. As a result, the ability to gather traffic statistics to see when traffic patterns change, e.g. whether a DDoS attack is over,

For more information about Blackholing, see https://www.de-cix.net/en/services/blackholing.

is lost. The Blackholing Advanced mechanism solves this problem by allowing the customer to shape the traffic routed to the blackholed prefix (https://www.de-cix.net/en/services/blackholing-advanced). Thus, it is still possible to inspect a portion of the traffic while protecting the infrastructure from congestion at the same time. This visibility enables customers to announce and withdraw Blackholing routes in a more efficient way, optimizing the response to the DDoS attack.

Moreover, BGP customer announcements are checked against Internet Routing Registries (IRR) to prevent route hijacking and other attacks.

In a software-driven world, it is important to ensure security measures also on the application layer. For our customized software stack, we highlight two important methods:

1. Constructive Code Quality Assurance methods: for instance, during the development process we use the best practices of versioning workflows and continuous integration, thus ensuring an extensive code review process before deployment.

2. Analytical Quality Assurance methods: We consider analytical QA to be an important part of the process as well. For example, our software penetration tests are routinely carried out by external partners to detect any security vulnerabilities.

Moreover, DE-CIX employs a 24/7 monitoring solution to monitor different aspects of the network and to support software and hardware during operations. More specifically, we employ public smoke pings to monitor RTT to our customer routers. We have recently expanded our monitoring system in that we are employing additional measuring points (probes) that help us to understand and to solve problems faster and more efficiently in the case of a malfunction. For example, we monitor the reachability of routers and line cards, CPU utilization, and the utilization of interconnection between routers. We also collect additional statistical data that is shared with our customers, e.g., customer port utilization, reachability of the customer hardware, temperature in data centers, etc.

This statistical data is available for our customers in the DE-CIX portal (https://portal.de-cix.net/).

Resilience mechanisms – redundancy as a top priority

To ensure the flawless operation of our platforms 24/7, solely employing security mechanisms is not sufficient. For this reason, numerous resilience measures are also defined and enforced. Our resilience efforts rely on creating redundancy on all levels of our infrastructure, such that in the case of unforeseen events (e.g., natural disasters, power outages, floods, or fibers cuts) our platform remains unaffected, or operations can be restored in minimal time. More formally, resilience can be defined as "the ability of an organization to prevent or resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event" (according to ISO 22300 (2012)). In the following, we describe various resilience measures that are in operation at DE-CIX.

L1: Generally, DE-CIX follows N+1 redundancy principle in all bigger interconnection platforms. For example, the DE-CIX Apollon interconnection platform in Frankfurt, the largest of the DE-CIX locations, consists of four core routers. These are indirectly connected via edge switches. These cores are built in four different data centers, one of which is for redundancy purposes – if the three others fail or if there is a sudden increase in traffic volume, we the additional data center in which we operate the fourth core router has spare capacity. Our Apollon platform in New-York, as another example, has two cores.

All our routers are equipped with a redundant power supply for emergency purposes, in case the primary one fails. When planning our networks, we always ensure redundant cabling in case of failures, with at least two geographically independent fiber optic cable paths.

Additionally, we have the following redundancy measures in place:

- Routers (NOKIA 7750 SR-s, 7950 XRS (e), 7250 IXR series) redundancy for cooling N+1; power supply 1+1; two control planes for high availability 1+1; fully geo-diverse and redundant circuits for all our interconnected Internet Exchanges
- Patch robots 2+1 redundancy
- Subsea cables 1+1 redundancy

L2: Switches and routers employ Link Aggregation Groups, meaning that multiple physical links are aggregated into one virtual link (one MAC address) and there is added redundancy. Additionally, we have MPLS Path Failover with 1+1 redundancy.

L3: The route server setup also consists of three devices for redundancy purposes (for the purposes of maintenance). There are three route servers for each protocol, IPv4 and IPv6, and additionally three blackholing route servers.

L4-7: When designing software, we follow three main principles to accommodate resilience:

1. Isolation: Separating components, such that unexpected errors do not propagate and affect the whole software stack.
2. Loose coupling: Different components interact with each other asynchronously – if one hangs, the other one is not affected.
3. Redundancy: We implement redundancy already in the design phase, for example by using microservice architecture.

We monitor all of our systems and if any irregularities – such as bugs or outages – are registered, our technical team (which is available 24/7/365) is notified in accordance with our escalation plan. For catastrophic and disastrous events, we have recovery plans in place.

DE-CIX organizational measures

Since 2010, DE-CIX has a security management system that is ISO 27001 certified based on the German Federal Office of Information Security baseline protection (“BSI IT Grundschutz”). This methodology helps us to implement information security measures.

To fulfill the requirements of an essential service and recommendations of ISO 27001, we follow three main security goals which apply to all data which is handled by our systems: confidentiality, integrity, and availability. Our Corporate IT Security department manages the processes internally based on the ISO 27001 baseline protection and

ensures any operational IT security task in this context is carried out according to the defined procedures.

Other organizational measures in place at DE-CIX:

- Two factor authentication, emergency documentation
- Customer service team on-call 24/7/365
- Abuse management processes

To support Internet security, DE-CIX is also one of the ten founding participants in the MANRS (Mutually Agreed Norms for Routing Security) initiative. MANRS was initially established by and for network operators, but Internet Exchanges also play a vital role in Internet security. The MANRS IXP Program includes a set of security actions, such as filtering prefixes according to IRR and RPKI, to address the unique needs and most significant threats for Internet Exchanges.

Security and resilience are at the heart of DE-CIX

As a representative of critical infrastructure, DE-CIX is a critical part of the global Internet infrastructure and is thus prepared for different types of threats. Security has always played an important role at DE-CIX, and we take proactive action to always be prepared and to deliver highly secure and resilient interconnection platforms.

DE-CIX

About DE-CIX

As the leading Internet Exchange operator and interconnection provider, we help companies to realize new opportunities and future-proof their connectivity needs to manage growing data volumes and new applications. From easy and secure cloud connection to creating interconnection ecosystems, we make interconnection easy. Anywhere.

Want to know more?

Visit de-cix.net
Email sales@de-cix.net