2023
GLOBAL STATE OF CYBERSECURITY STUDY

infoblox®

With a broadband connection in nearly every household, The Netherlands is regarded as one of the most wired countries in the world. But that **ubiquitous connectivity also makes the nation a bigger target for malicious cyber activity**. Survey findings over the past 12 months reveal what types of attacks organisations in The Netherlands have been facing, how they responded and what will be top of mind as 2023 unfolds.

THE NETHERLANDS

63%

Of Dutch organisations suffered one or more breaches from unpatched DNS, DHCP or IPAM networking servers; remote, employee-owned endpoints; IoT devices or networks
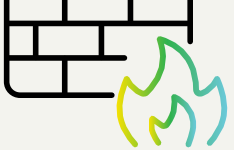
AVERAGE NUMBER ATTACKS PER ORGANISATION BY TYPE

45 email/phishing   **18** device/endpoint

27 network   **15** application

HOW DUTCH ORGANISATIONS RESPONDED IN THE WAKE OF COVID-19

46% Accelerated digital transformations to support remote workers

36% Added resources to their networks and databases

32% Hired more IT staff

TOP SECURITY TECHNOLOGY SOLUTIONS

71% Added new VPNs or firewalls

43% Added remote corporate-owned mobile devices to their networks

31% Added cloud-managed DNS-DHCP-IPAM servers to harden security

---

BIGGEST
CHALLENGES

1. Shortage of IT security skills

2. Difficulty monitoring remote worker access

3. Proliferation of siloed security tools

MOST URGENT THREATS FOR NEXT 12 MONTHS

39% Data leakage

37% Ransomware

33% Direct attacks through cloud services

32% Attacks exploiting remote-worker connections

> "I believe our biggest threat is the amount of people that have no idea how cyber security works"
>
> –IT security consultant, Dutch technology provider

> GET THE FULL REPORT

Complete insights and top cybersecurity issues and priorities for the coming year are available in the full **2023 Global State of Cybersecurity Study: The Netherlands**

2023 GLOBAL STATE OF CYBERSECURITY STUDY
THE NETHERLANDS

CRA

Survey findings were conducted by the CyberRisk Alliance and underwritten by Infoblox.