The nature of cybersecurity: Be resilient to thrive

The threat landscape is continuously changing, especially during these tumultuous times. In such a dynamic environment, and with absolute security as an impossible goal, businesses must be ready for anything.

About the Report

Speak to our experts

Our cybersecurity experts can help you understand your current risk profile to chart your future security strategy, and help to manage, monitor and optimize your security posture.

Technology remains at the top of the list of most-attacked industries.

The most common techniques observed globally were remote code execution (15%) and injection (14%) attacks.

About 20% of all attacks targeted CMS platforms over the last year.

Botnets such as Mirai, IoTroop (Mirai variant) and Echobot have advanced in automation, improving their propagation capabilities.

2019 was a year of enforcement … but GRC is becoming more complex and challenging to navigate.

Organizations are not following patch-management best practices.

Technology was the most attacked industry accounting for 25% of all attacks (versus 17% last year).

Apache software was the third-most targeted in 2019, accounting for over 15% of all attacks.

Government sector targeting driven by geo-political activity at 16% (versus 9% last year).

New regulations are being implemented or are coming soon.

Nearly 55% of all attacks were application-specific (33%) and web-application (22%) attacks.

Maturity of processes

Executive support

Key data-driven insights

1. Threat actors are innovating

Threat actors are innovating.

2. IoT expropriation

Technological advances transform both IoT devices and traditional infrastructure, creating opportunities (15%) and threats (14%) alike.

3. Old vulnerabilities remain an active target

The difference between current and target state is one driven by aspiration, where they need to be. Many business drivers, including cost, compliance and resources may result in achieving less than the desired goals.

In order to close the gap, each of these industries must ensure a constant focus is placed on:

- Industry hotspots
- CISO
- Industry hotspots
- Executive support
- Industry hotspots

4. Content management systems (CMS) are at risk

There’s a gap between current levels of attainment and the expectations of several industries.

5. Evolution of governance, risk and compliance (GRC)

The difference between current and target state is one driven by aspiration, where they need to be.

Many business drivers, including cost, compliance and resources may result in achieving less than the desired goals.

In order to close the gap, each of these industries must ensure a constant focus is placed on:

- Industry hotspots
- CISO
- Industry hotspots
- Executive support
- Industry hotspots

6. Shift in sector targeting

The difference between current and target state is one driven by aspiration, where they need to be.

Many business drivers, including cost, compliance and resources may result in achieving less than the desired goals.

In order to close the gap, each of these industries must ensure a constant focus is placed on:

- Industry hotspots
- CISO
- Industry hotspots
- Executive support
- Industry hotspots

About the Report

Contains global attack data gathered from NTT Ltd. and supported operating companies from 1 October 2018 to 31 September 2019.

Analysis is based on log, event, attack, incident and vulnerability data from:

- Over 150 Cybersecurity Advisory assessments
- Over 7,500 security clients on six continents
- 25% compared to in 2018
- 300+ SOCs
- 7 R&D centers
- Global Threat Intelligence Platform

Speak to our experts

Our cybersecurity experts can help you understand our current risk profile to chart your future security strategy, and help to manage, monitor and optimize your security posture.

Find out more about our Intelligent Cybersecurity solutions and services

Get the 2020 Global Threat Intelligence Report here