Cybersecurity Forecast 2024

Check out the five biggest trends that Google Cloud security experts anticipate.

AI will have a major impact on cyber operations and security.

- More sophisticated and scalable phishing campaigns, phishing and SMiSh threats could be harder to spot with newer phishing and grammar errors.
- With access to info like names, companies, and job titles, attackers could use AI to more easily target more people with personalized attacks based on them.

More description in reads
A clever AI prompt will be used to create new laws, despite photos, videos, and fake news, and more. As this content enters the news cycle, people may become less critical of news and like it online.

An-powered attacks will meet with AI-powered defenses.
- With AI, organizations will be able to analyze input data and detect and respond. Defenders will also be able to analyze large data sets and detect the target. They need to take immediate action.

Nation states will conduct cyber operations for geopolitical gains.

- China
Cyber activity from China is expected to continue to be driven by long-term national goals, regional issues, and economic influence over key sea routes.

- North Korea
North Korea is expected to continue to place heavy emphasis on conducting cyber crime, notably targeting power systems and fund siphoning as well as military and nuclear programs.

- Iran
Protests including geopolitical ambitions, economic development needs, and competition with regional rivals will be key drivers of Iran's stated cyber activity in 2024.

More description in reads
Although Iran's cyber espionage operations have not yet shown up, we've seen an increase in zero-day attacks in recent years.

- Russia
Alongside intelligence gathering and digital warfare forays on Ukraine, there could be more cyber espionage attempts with Russian long-term geopolitical goals, as well as for profit.

There will be more zero-day attacks and use of other techniques to evade detection.

- More targeting of fend-to-monitor edge devices and virtualization software
- A new kind of attack targets the modern fabrication process for security chips
- Cryptography groups to create "deeper, more extensive internet of things," and of life, devices, and nodes.

There's been a steady increase in zero-day attacks since 2016, but N2023 or N2024 we expect more zero-day attacks to both nation-state attackers and cyber criminal groups.

More description in reads
Attackers will need to be as sophisticated as we can to keep their geopolitical goals.

There will be a rise in cyber activity around major global events.

- In addition to hangout breaches related to Olympic events, it's likely that attackers will use a range of tactics to target elections around the world and the Summer Olympic Games in Paris.

For the upcoming U.S. presidential election, we expect cyber activity such as espionage and influence operations targeting elections and voting systems.

We also anticipate seeing similar cyber activity around European Parliament elections, as well as elections taking place in Taiwan, South Korea, India, and Indonesia.

The way malware is developed will change.

Malware will be expected to continue developing using modern programming languages such as Go, Rust, and C. These languages are safer and more secure than older languages, enabling faster development of complex malware that is easier to create and harder to detect.

We also anticipate:
- More targeting of I2M-to-monitor edge devices and virtualization software
- A new kind of attack targets the modern fabrication process for security chips
- Cryptography groups to create "deeper, more extensive internet of things," and of life, devices, and nodes.