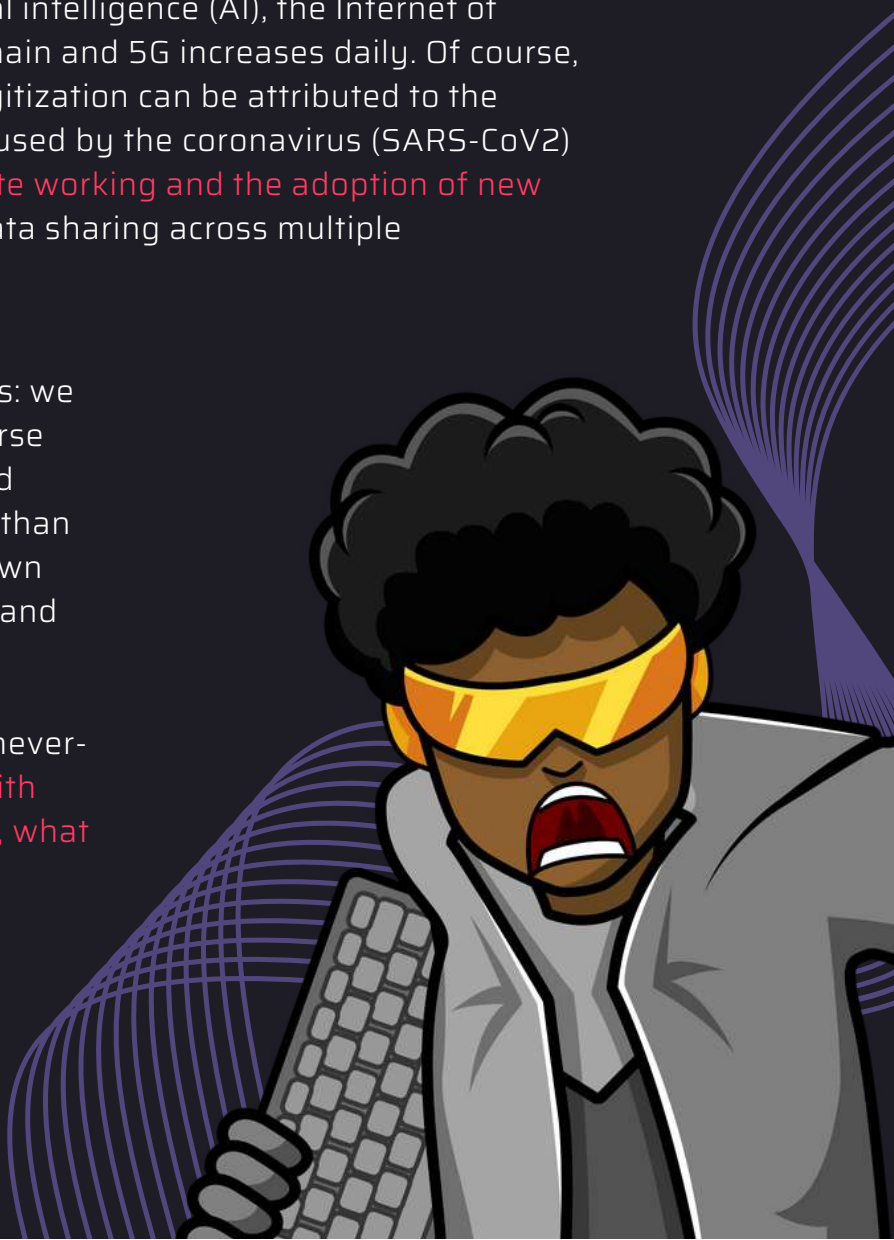
HACK3R_
RANGERS

CYBERSECURITY IN THE AGE OF TECHNOLOGICAL DEPENDENCE

The world is addicted – and no, we're not talking about illegal psychoactive substances. We are talking about technology. Every sector of society (end users, businesses and governments) is marching towards a future increasingly dependent on technological innovation. Every day, an array of new solutions, tools and protocols emerge, in preparation for a new era of a decentralized Internet.

The appetite for concepts like artificial intelligence (AI), the Internet of Things (IoT), edge computing, blockchain and 5G increases daily. Of course, part of the blame for this rampant digitization can be attributed to the accelerated digital transformation caused by the coronavirus (SARS-CoV2) pandemic. The crisis has driven remote working and the adoption of new business models that permit wider data sharing across multiple environments.

And there's no stop to the innovations: we are already talking about the metaverse and a possible future where we spend more time in a digitized environment than in the real world. This future has its own economy, based on cryptocurrencies and non-fungible tokens (NFTs), causing unprecedented disruptions in socio-economic experiences, coupled with never-before-seen virtual immersion. But with this rise in technological dependence, what becomes of our cybersecurity?



HACK3R_
RANGERS

The other side of the coin

Increases in cyberattacks

Naturally, all this innovation creates more room for attacks and the statistics don't lie: the increased reliance on ever more complex digital systems is diminishing our ability to respond to cyber threats. Think back to 2020; no less than USD 406 million was transferred to ransomware cryptocurrency wallets – a fourfold increase compared to the previous year, at "only" USD 93 million.

And it’s no wonder. Even though technological innovations make our lives a lot easier, they can also be manipulated by cybercriminals. One "business model" that has already proven profitable is ransomware-as-a-service (RaaS), allowing a complete layperson to license malware and digitally hijack a company. The profits are split with the operators and the victim is left to fend for themselves.

Ransomware is also increasingly aggressive and targeting weak points. Besides simply encrypting files, they have moved on to double or even triple extortion, threatening to release compromised data or launch DDoS (distributed denial-of-service) attacks against the victimized server. Additionally, the most common targets have become critical infrastructure, which cannot afford to halt operations for even an hour. As a result, the pressure to just pay the ransom is even greater.

HACK3R_
RANGER5

Of course, digital hijacking is not the only threat that comes with increased reliance on technology. There has never been more talk of attacks against the supply chain, and there's a reason: it, too, has been digitized. We increasingly rely on technology partners to keep companies running smoothly, which can lead to some rather delicate situations.

When the set of vulnerabilities in Log4j – an open-source library used by thousands of applications around the world – was discovered, analysts recorded more than 100 attack attempts per second. Cybercriminals have realized that it's ultimately easier to poison the source of the water than to poison each glass – and the need for ever-greater interoperability among systems means that the poison spreads with dizzying speed.

HACK3R_
RANGERS

Future concerns

What should we focus on?

In the Global Risks Perception Survey (GRPS), respondents ranked "cybersecurity failure" as one of the top ten worsening risks in the wake of the COVID-19 crisis. In addition, 85% of the World Economic Forum (WEF) leadership community considered ransomware the most dangerous and fastest-growing threat to public safety.

To make matters worse, there's the much-talked-about talent shortage. It is estimated that more than 3 million cybersecurity professionals are needed globally to provide rapid responses to threats, protect systems and raise awareness of best cyber hygiene practices. Fraud and disinformation campaigns are also showing worrying growth, with the use of deepfakes making scams even more realistic.

And for anyone who thinks that the situation can't get any worse: it is estimated that 40% of the global population is still not connected to the Internet. This portion, which already suffers from unequal rights, will become an even weaker community against the cyber threats emerging from a decentralized Internet and a highly digitized economy.

HACK3R_
RANGERS

Resolutions for a safer society

Statistics also show that companies are operating in a landscape where 95% of cybersecurity issues are considered the result of human error and 43% of leaks are caused – intentionally or not – by insiders.

As our technological dependence increases, all participants in this ecosystem must work together to define norms and rules of behavior that ensure the security of the new Web 3.0. To mitigate risks, greater cooperation is required among organizations, both to share threat intelligence and to work on initiatives focused on new trends – like blockchain, quantum computing, A.I. and the metaverse.

Within corporations, more open dialog between different departments and greater involvement of senior management (board and C-levels) are essential to optimize our security strategies. Only then will we move towards a future with less fragmentation and greater resilience in technological systems, which, inevitably, will be increasingly present in our lives.

The Hacker Rangers platform leverages the principles of gamification to create a dynamic, updated, and enjoyable educational environment in which your staff will be genuinely motivated to learn about safe behavior on the web. Through this approach, you can ensure a profound behavioral and cultural change, ultimately reaching the highest levels of cybersecurity maturity.

TEST OUR PLATFORM FOR FREE
FOR 15 DAYS!

HACKERRANGERS.COM

HACK3R_
RANGERS

References
The Global Risks Report 2022 (World Economic Forum, janeiro de 2022)