LINK11

WHITEPAPER

Algorithms vs. attackers: how AI strengthens cyber resilience

www.link11.com

Dear readers,

At a time when digital innovations are transforming the business landscape faster than ever, we are facing an unmistakable reality: the security of our IT systems and data is not just a challenge, but a strategic necessity. Cyberattacks are becoming more complex, more sophisticated methods are being used, and attackers are becoming increasingly professional.

It is therefore essential to be proactive and view cybersecurity as a competitive advantage. This white paper looks at how Artificial Intelligence (AI) can act not only as a challenge, but also as a critical tool in cybersecurity strategy. It is time for us to shape the future of cybersecurity together and strengthen the resilience of companies with the most innovative solutions.

I wish you an exciting read,

Best regards
Jens-Philipp Jung, CEO, Link11

Table of Contents

Introduction

The launch of ChatGPT in November 2022 marked a significant milestone in the development of AI by giving generative AI (GenAI) a huge boost. In just a few years, it has already been heralded as the technology of the future and has the potential to significantly increase productivity worldwide.

The impact of GenAI is profound. By 2030, around 30% of current working hours could be automated by technologies such as generative AI[1]. Rapid adoption could boost productivity growth by up to 3% per year. It is therefore no wonder that the demand for GenAI in particular, but also for machine learning (ML) and other AI applications, is growing exponentially.

Artificial intelligence, such as machine learning, plays a crucial role in the early detection of cyber threats. By analyzing large amounts of data, it can identify anomalies and suspicious behavior in networks or systems, enabling rapid responses and effective countermeasures. IT security solutions are increasingly using automation through AI to identify and close potential security gaps. This includes the automatic prioritization of security updates as well as the continuous monitoring and adaptation of security measures to new threats.

The majority of IT managers believe that cyberattacks have become more sophisticated and that attackers have become much more professional. Many do not feel adequately prepared for the new threat vectors, especially AI-based attacks. Increasing global tensions and cyberattacks are also a concern for German CEOs.

According to the PwC Global CEO Survey, 42% of German CEOs believe their company is at high risk from cyber threats in the next 12 months. On a global level, the figure is only 21%[2].

Criminals are using AI for example to make phishing emails more effective and steal business-critical information, while security providers are using AI to detect and block these threats. This constant arms race requires a proactive approach to security that includes both advanced defenses and basic risk mitigation best practices.

With a global shortage of over three million cybersecurity professionals[3], automation of cybersecurity operations is critical. It enables highly specialized talent to be deployed more efficiently while increasing the ability to respond to threats that require specific expertise. According to PwC's Digital Trust Insights[4], companies around the world are now recognizing the critical nature of managing cyber risk and its role in business success, leading to an increase in planned investment in cybersecurity.

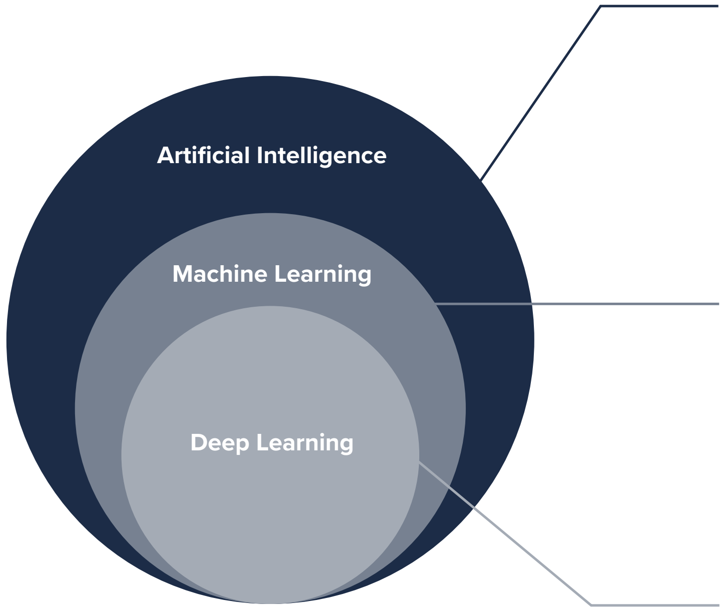
The rapid development of AI has far-reaching implications for the cybersecurity landscape. Attackers are using AI to increase the sophistication and effectiveness of their attacks, while defenders are using AI to automate and improve their security measures. This white paper highlights this dynamic relationship and emphasizes the need to invest in advanced technologies. At the same time, organizations should develop a robust risk management framework to take full advantage of AI while raising security standards.

> *By investing in AI and modern cybersecurity measures, companies can enhance their resilience and gain a competitive edge in today's digital landscape.*
>
> **Jens-Philipp Jung, CEO, Link11**

What is AI?

In the field of AI, scientists develop and use methods to create machine systems that solve complex problems independently. These systems take over decision-making processes that traditionally required human intelligence. AI uses techniques such as machine learning (ML) and deep learning (DL) to recognize patterns in large data sets and make decisions based on them.

Forms of artificial intelligence



Artificial intelligence:

Artificial intelligence (AI) simulates human intelligence with machines, especially computer systems. This includes learning (the collection of information and rules for using the information), reasoning (the use of rules to draw approximate or final conclusions) and self-correction. Special applications of AI are expert systems, speech recognition and machine vision.

Machine learning:

Machine learning (ML) is a branch of artificial intelligence. By recognizing patterns in existing data, IT systems are able to independently find solutions to problems.

Deep learning:

Deep learning (DL) is a sub-area of machine learning and uses neural networks and large amounts of data. The learning methods are based on the way the human brain works and result in the ability to make predictions or decisions.

The term "AI" was coined in 1956 at a conference of leading scientists at Dartmouth University, including the American computer scientist and founding father of AI, John McCarthy. AI has continued to develop in parallel with the increase in computing power and database technologies. Today's systems can process enormous amounts of data in real time and are particularly responsive. There are currently three types of AI:

- **Weak artificial intelligence (Weak/Narrow AI):** Specializes in singular and goal-oriented tasks such as character, text or face recognition, internet search engines, and navigation systems.
- **Strong artificial intelligence (Strong/General AI):** Theoretically capable of mastering intellectual tasks like a human. For example, an AI that was originally developed to extract text from an image could also extract text from a video without additional training. However, such tasks require advanced computing capacities and therefore this level has not yet been reached.
- **Artificial superintelligence (Super AI):** A theoretical vision of the future in which AI would be able to improve itself, set its own values and goals, and adapt these to different situations and environments.

From online retail to IT security: a wide range of possible applications for AI

Applications of AI in everyday life	Applications of AI within business	Applications of AI in cybersecurity
Personalized recommendations in online retail	ML algorithms analyze data for chatbots and autonomy	Threat detection and mitigation in real time
Voice assistants such as Amazon Alexa and Siri	Use of Deep Learning for facial and voice recognition	Detection and defense against malware and phishing attacks
Improved online translator through neural machine translation	Virtual support agents provide IT support and automate tasks	Automated analysis and response to security incidents
Facial recognition for smartphones and security applications (Face ID)	AI improves planning, maintenance, and automation in the supply chain	Identity and access management
PayPal fraud detection	AI identifies new leads and optimizes sales processes	Transaction monitoring and fraud detection
Use in medicine and care	Real-time personalization and optimization of campaigns	Protection of data and personal information
Autonomous vehicles and intelligent driver assistance systems	Virtual assistants provide proactive customer service and quality control	Ensuring the integrity and confidentiality of data

From Turing to ChatGPT: The most important moments in the history of artificial intelligence

Some highlights in the development of artificial intelligence are:

1950s
The birth of AI, when the first algorithms based on electrical circuits were developed. This marks the beginning of research and theoretical conception of artificial intelligence.

1970s
After the initial hype surrounding AI, which was characterized by ambitious expectations, the "AI winter" began, during which research funding was cut and interest waned considerably. This period was characterized by disappointment and a lack of progress.

1997
A significant moment when IBM Deep Blue, a chess computer, defeated the reigning world chess champion. This was the first demonstration of the capabilities of AI in a specific application area and received a lot of media attention.

2010s
A renaissance for AI, supported by advances in hardware and the availability of big data. This period was characterized by significant breakthroughs in the field of machine learning and the deeper integration of AI into various applications.

2013
The startup DeepMind developed an AI that learned to play Atari software on its own. This was an early indication of AI's ability to master complex tasks through autonomous learning.

2015
A Deep Neural Network from Microsoft Research achieved the same error rates in image recognition as a human. This marked a significant advance in visual perception by AI.

2016
Google DeepMind developed AlphaGo, an AI that defeated the world's best Go player, highlighting AI's ability to solve strategic and complex problems in a gaming context.

2022
OpenAI caused a worldwide sensation with ChatGPT, an intelligent language model that can hold natural human conversations. This took AI to a new level of language processing and understanding.

Threats for artificial intelligence

The integration of AI systems promises more efficient processes, better decision-making, and new possibilities in automation. While the benefits and potential of AI are far-reaching, there are considerable dangers lurking in its use, particularly through specialized attack vectors that exploit vulnerabilities in AI systems.

Adversarial attacks have emerged as a serious threat to AI systems. These attacks aim to undermine the integrity and functionality of AI models through targeted manipulation of input data. Attackers can use specially crafted inputs to trick the model into making incorrect predictions, significantly reducing the effectiveness of the AI.

The main types of adversarial attacks include the introduction of erroneous data during the training process (**data poisoning**), the targeted falsification of inputs to elicit certain reactions from the model (**model evasion**), and the extraction of sensitive information about the model itself or its training data (model extraction).

Another security risk is **backdoor attacks**. These begin with the manipulation of training data **(poisoning)** to later cause targeted wrong decisions as soon as a certain **backdoor trigger** is present in the input. Without this trigger, however, the behavior of the model remains unchanged. To protect against such attacks, pre-trained models should only be obtained from trustworthy sources, transferred securely, and have their integrity checked. Documentation of the training data and existing protective measures against data manipulation are also essential.

In addition, **prompt injection attacks** bypass security measures by injecting malicious commands into user input to gain control of the system. Finally, **inversion and model stealing attacks** pose a threat by exposing the sensitive data and functionality of the AI by drawing conclusions from training data or through targeted **reverse engineering**.

These diverse threats emphasize the need for robust security strategies, continuous monitoring, and the application of proven safeguards to ensure the integrity and reliability of AI-based security solutions.

Threat scenarios for AI: risks and vulnerabilities at a glance

Threats	Description
Data Poisoning	The training data of the AI model is manipulated to undermine the accuracy and reliability of the model. Attackers could inject malicious data into the training process to deliberately damage or corrupt the model.
Model Evasion	In these attacks, the AI model is evaded so that it does not recognize threats. Attackers use techniques to shape inputs so that they remain inconspicuous even though they are malicious. These attacks are often designed to bypass existing security systems by being classified as legitimate.
Model Extraction	In these attacks, attackers attempt to copy or steal the AI model by systematically analyzing inputs and the corresponding outputs of the model. This can lead to a loss of intellectual property and sensitive information while also allowing attackers to understand and manipulate how the model works.

Focus on the IoT: Prof. Markus Miettinen on AI-supported cyber security and the future of networking

Prof. Dr.-Ing. Markus Miettinen, Frankfurt University of Applied Sciences, in conversation with Lisa Fröhlich, company spokesperson at Link11

Prof. Miettinen, what are your main areas of research?

I research systems that detect attacks against IoT devices. IoT devices are increasingly permeating our everyday lives, from smart homes to industrial processes and intelligent infrastructure. However, many of these devices have security vulnerabilities that make them susceptible to attacks. We use AI models to determine the normal communication behavior of the devices and identify deviating behavior as a potential attack.

How is your research related to AI?

A big problem with AI models is that they only work properly if they are trained with correct data. If an attacker manipulates the training data or the training process, the AI model can produce incorrect outputs. That's why I'm researching methods to detect and eliminate such manipulations.

How has the cyber threat landscape evolved over time and what new challenges are relevant today?

Cyberattacks have become more professional, with criminals looking for profit and state actors using cyberattacks as part of their offensive potential. A particular challenge today is the increasing connectivity of the IoT. Many of these devices have inadequate security designs and are vulnerable to attacks, which exacerbates the threat situation.

Why is cybersecurity so crucial in today's digital world?

Cybersecurity is crucial because almost all social processes are digitized - from administration and business transactions to cultural offerings and communication. The role of cybersecurity is to secure our digitized processes and systems against attacks and to ensure the resilience of AI-powered systems against tampering.

How do cybercriminals use AI technologies to make their attacks more effective?

Cybercriminals use AI to optimize their attacks. For example, AI models can generate parts of malware and compose spam emails that make it easier to deceive users due to their high quality. Even with smaller languages such as Finnish - my mother tongue - it is no longer easy to tell whether an email is genuine or a scam.

What role does AI play in preventing cyberattacks?

We can use AI to learn how IoT devices normally behave and communicate. If a device is under attack, we can detect this based on its deviating communication behavior. The system learns independently what is normal and what is not normal and works autonomously.

Will there be more regulation?

There will certainly be efforts to regulate the use of AI to prevent unfair practices and take ethical issues into account. Security research is hot on the heels of the attackers and is also conducting independent research in order to be one step ahead of them in the best-case scenario.

Thank you very much for the exciting insights.

How criminals are already using AI today

If your company's IT has not yet been the target of a large-scale attack by criminals, you have simply been lucky. There is a saying among experts that there are only two types of companies: Those that have already been through a major hacker attack, and those that don't know they've already been attacked.

Criminals and hackers are following the development of AI just as closely as legitimate companies. And just like them, they are taking advantage of this technology. Companies should not be led by the misguided idea that AI is too complex or too expensive for criminals. After all, cloud providers such as Google, Amazon and Microsoft already offer interfaces to computing systems for machine learning. It should also not be forgotten that competitors, intelligence services, and states can also be behind attacks from the internet. In such cases, money plays a subordinate role.

There is a whole range of scenarios for the use of AI by criminals, e.g.:

- **Biometrics:** Several impressive examples show that AI can be used to virtually create deceptively real-looking people and faces. As a basis for such "deep fakes", the systems can use everyday photos of the people concerned. In this way, biometric security systems based on facial recognition can be overcome.
- **Speech recognition and speech synthesis:** Applications that could generate speech artificially are similarly sophisticated. Google, for example, has developed a voice computer that can handle telephone appointments on request. Callers do not realize that they are talking to a computer system. Using "natural language generation", attackers can imitate the voice and tone of a trustworthy person and thus gain access to potentially sensitive information. Conversely, voice recognition and speech analysis can be used to extract data from telephone recordings or other sources of information that reveal details about security systems or provide information about upcoming transactions, which can then be intercepted.
- **Machine learning:** Machine learning is used by attackers to better analyze the behavior of potential victims from a company's large amounts of data. The aim is to develop promising phishing attacks. However, machine learning can also be used to analyze vulnerabilities in the security systems used. Machine learning makes it possible to program malware that can only be traced back to a very limited extent, if at all. One attack scenario would be "self-learning" Trojans.
- **(Predictive) analytics:** AI systems are often used to make predictions. Based on data already obtained from successful and averted attacks, intelligent systems can support the attacker in developing a strategy for a promising attack. An AI system can also automatically identify vulnerabilities in IT systems.
- **Generative AI:** Criminals could use generative AI such as ChatGPT and other Large Language Models (LLM) to create very convincing phishing emails. Additionally, the models can assist in the development and customization of malware.

The following threats are currently among the most serious

Automated phishing attacks:

Using AI, attackers can create highly personalized phishing messages tailored to the target's social media and communication patterns.

AI-generated malware:

AI is changing the landscape of malware development. AI-generated malware can adapt to the environment and change its behavior, overcoming traditional detection methods.

Deepfake technology:

AI creates deceptive fake images, videos and audio recordings that are used for social engineering and information manipulation. For example, a fake video call from a CEO could prompt an employee to transfer money or disclose sensitive information.

AI-driven reconnaissance:

Attackers can use AI to identify vulnerabilities and potential targets within a network more quickly and accurately. This automated reconnaissance enables targeted attacks on specific systems or individuals that provide valuable information or access.

Autonomous weapons and DDoS attacks:

AI-driven autonomous systems can be used to create botnets that can carry out DDoS attacks. These systems autonomously identify vulnerable devices and use them to overload networks and make services inaccessible.

AI-generated code as a security risk:

AI can be used to automatically generate or optimize code. This carries the risk of creating faulty or malicious code that introduces security holes or vulnerabilities into software applications or systems. Faced with these overwhelming technical possibilities and the resulting concrete threat from cybercriminals to digital business processes, companies should also rely on AI to defend against threats.

Data leakage through compromised AI models:

Compromised AI models can intercept sensitive data or provide incorrect results, which can result in data breaches.

In view of these overwhelming technical possibilities and the resulting concrete threat to digital business processes from cyber criminals, companies should not hesitate to rely on AI to defend against threats.

Attacker or defender? Prof. Stjepan Picek on the future of AI in IT security

Dr. Stjepan Picek, Associate Professor, Radboud University,
in conversation with Lisa Fröhlich, company spokesperson at Link11

Could you please briefly tell us about your research in the field of cybersecurity and AI?

My research deals with both AI for security and the security of AI. As the head of the AISyLab group, we explore approaches such as deep learning-based side-channel analysis, AI-assisted fault injection, and backdoor attacks on neural networks. Our work includes centralized and decentralized learning paradigms such as federated learning and split learning.

Why is there so little differentiation in public when it comes to AI?

AI is a huge field. There is a lot of interest in deep learning, a subfield of machine learning. Most of the news that reaches a general audience makes it difficult to grasp the entire field of AI.

How do you assess current developments in the field of AI and its role in cybersecurity?

AI is increasingly being used for both attack and defense. Developments in deep learning enable the processing of huge amounts of data and more accurate predictions. I believe that this is where we will see the most developments in the next few years: using more data and achieving more accurate results.

What challenges do you see?

As we are constantly developing new AI technologies, it is of course realistic that there will also be attacks on these new AI technologies.

What IT security threats is AI exposed to?

Like other systems, AI is also exposed to various IT security threats and can be classified according to the CIA triad (confidentiality, integrity, availability). One major difference is that AI has increasingly become the focus of public attention due to its current hype, while other threats are often only considered by specialists. Nevertheless, AI is not immune to attacks and must be secured accordingly.

How do you see AI developing in the field of cybersecurity in the future?

It's difficult to predict because AI is developing so quickly. We will see more attacks on new AI systems and more approaches to fully automated defense. Generative AI and large language models will keep the research community busy over the next few years.

Who is ahead in the race between attackers and defenders and why?

I would say the attackers. Many AI systems are easy to attack, while defense is difficult and expensive. For every reported malicious use of AI, there are probably many unknown ones, which makes it difficult to evaluate properly. Furthermore, a defense against one attack says nothing about the security of AI systems against different attacks.

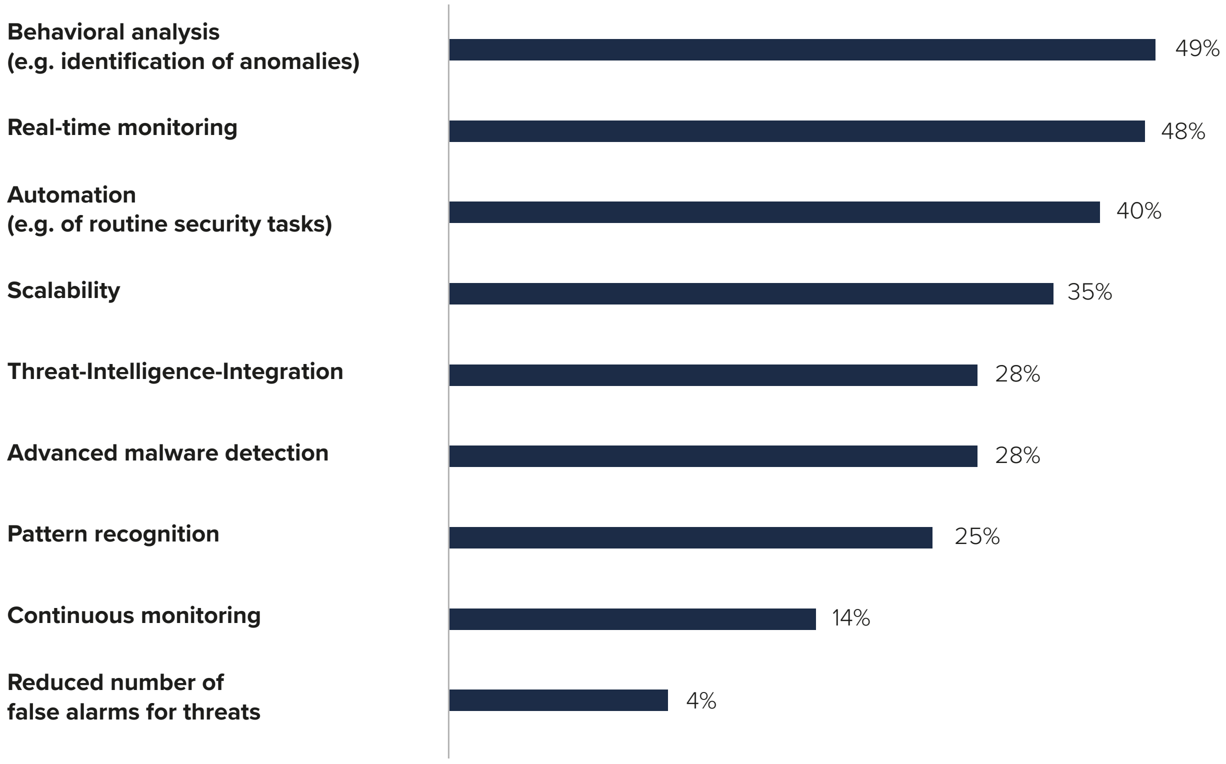
What support can AI offer against cyberattacks?

AI is already widely used, either in defense mechanisms, such as malware and spam detection, or intrusion detection. In addition, security experts can use AI to take on the role of the attacker to test the security of systems. It is also possible that more powerful AI models will help to defend against attacks by enabling faster detection and prevention of attacks, thereby at least reducing the need for human experts.

Thank you very much for the interesting interview.

The results of the latest Capterra Security Report[5] show exactly where AI models can help defend against attacks:

How AI improves threat detection and response compared to traditional cybersecurity methods



Source: Capterra Security Report
Question: How does AI improve threat detection and response compared to traditional cybersecurity methods? select all that apply. n: 670
Note: Since there were multiple answer choices, the total may exceed 100%

> "The future of cybersecurity lies in intelligent automation. AI-supported systems not only offer round-the-clock protection, but also learn independently to recognize and fend off threats in real time."
>
> **Karsten Desler, CTO, Link11**

Cyber resilience is becoming increasingly important

In an increasingly digitalized business world, cyberattacks often lead directly to business interruptions. According to the German industry association Bitkom, this causes around 150 billion euros per year in damage to the German economy[6]. Strengthening the resilience of IT infrastructure is therefore an increasingly important priority.

To this end, concepts are being developed and measures defined to ensure the continuation and resumption of business activities during and after a cyberattack. The aim of cyber resilience is to be well prepared and able to react quickly to security breaches and counteract security incidents while maintaining control of the business.

Resilience to external attacks stands and falls with the security culture practiced in the company and the protection solutions used. Both require permanent adjustments to security concepts and control solutions. A static approach in which processes and protection solutions are defined once is no longer sufficient in view of the highly dynamic security risks.

Those who invest cleverly in new technologies can disproportionately increase their level of resistance. According to the results of Accenture's State of Cybersecurity Resilience 2023, companies that embed cybersecurity measures experience a digital transformation that is almost six times more effective than those that do not. As a result, they not only strengthen their cyber resilience, but are also 18% more likely to increase their revenue growth[7]. AI and machine learning are seen as the technology of the future.

AI is superior in attack defense

AI is a neutral technology that is neither good nor evil at its core. In the hands of criminals, it poses a serious threat, but conversely, it can also be used to defend against threats. Attempts to combat threatening AI with human intervention are doomed to failure due to the technical differences in scale. In IT, security solutions benefit significantly from AI components to overcome the numerous weaknesses of traditional solutions.

1. AI is faster

As digitalization progresses, companies are now faced with the challenge of monitoring and securing a growing number of applications, external cloud providers, and devices. In the coming years, the number of systems to be monitored will increase steadily due to the Internet of Things (IoT). Intelligent sensors will take over the control of building technology, transmit information in the supply chain, or enable new business models. A billing model that is based on the specific use of devices (pay per use), for example, is inconceivable without sensors.

In turn, the amount of data processed by an organization will continue to grow, and the number of interfaces and communication channels within the company will increase. However, it is well known that every additional channel embedded in the IT landscape is also a potential gateway for political motivated and criminals. Automated AI systems that monitor data traffic from IoT sensors, for example, can detect anomalies in their behavior much more quickly. They raise the alarm or initiate countermeasures faster than a human ever could.

In large and possibly globally active companies, employees are logging into internal systems around the clock. Apparently too many to check them manually. In this context, AI can recognize peculiarities to react appropriately based on predictive analytics and pattern recognition. If an employee usually logs into a company system from a defined region during fixed working hours, a successful login in the middle of the night, from a different time zone or a completely different region, is at least suspicious. Detecting such an occurrence manually is like the proverbial search for a needle in a haystack.

2. AI overlooks nothing

Large-scale attacks require preparation and lead time. During this time, the attackers try to position as many systems or attack vectors as possible. In doing so, they leave traces on hijacked systems. Through pattern recognition and analysis, AI-based defense systems can detect even minor deviations. Administrators and security officers receive an alarm in good time if the system classifies an incident as a potential preparation for an attack.

If a DDoS attack is imminent, rapid action is required. But when is the network traffic still growing organically? When is an attack on the horizon? AI also shows its speed in this context. Within seconds, regular analyses of growth, data sources, and the characteristics of a DDoS attack are carried out. The software is superior here, even to experienced employees, as it is faster at processing and analyzing multiple data sources and taking countermeasures.

Conventional detection system[8]
Software (SW) works with rigid models
SW generates decisions based on a transparent control system
SW is not capable of learning
SW uses signatures and correlations against different types of data

Recognition systems with learning / AI components
SW works with adaptive models
SW generates decisions on the basis of a gradual evaluation
SW learns continuously
SW learns complex patterns from a large amounts of data

3. AI is better than any patch

The defense against criminal attacks often resembles a game of cat and mouse. Typically, security solutions differentiate between "good" and "bad" requests or program code. If new security vulnerabilities are discovered, the usual reaction is to make manual adjustments. A patch is applied, the rules in a firewall are changed, and malware signatures are updated.

In this way, security systems are brought up to date. However, the development of patches, updates and rules takes time and is based on incidents that have already occurred or security gaps that have been discovered. In the meantime, the criminals have already moved on. They use other networks for attacks that are not yet covered by the firewall, exploit new security gaps, or use so-called "polymorphic" malware. Their code is constantly changing to make the task of detection programs more difficult and to improve the malware's camouflage.

Analysis systems based on AI ensure equal opportunities against attackers. Self-learning AI systems, which continue to improve during use and thus make their own automated decisions, are powerful tools. In a "whitelisting" strategy, all network traffic is initially classified as malicious until the opposite is proven, for example by analyzing packet content. AI speeds up the analysis and uses a learning system to decide which data streams are allowed to pass.

4. AI overcomes workforce shortages

Across all sectors, three parallel developments in IT security have emerged in recent years, the combination of which gives cause for concern. The number of attacks against companies has increased. Phishing, successful attacks with ransomware, DDoS attacks: The threat situation has intensified. As already mentioned, this also because the number of potential gateways and platforms is growing.

At the same time, new regulations have been passed by politicians that have a direct impact on IT security. The GDPR and NIS2 describe very precisely what companies and authorities must do as part of "technical and organizational" measures to protect data from unauthorized access, manipulation, and theft. This means that the requirements for IT security are also increasing.

Implementing compliance and responding to increased threats therefore requires more specialist staff. The demand for IT security experts is very high. However, many companies, especially small and medium-sized ones, are unable to recruit these specialists. There is a pronounced shortage of specialists in this segment[9].

As expected, this has consequences: Existing staff are overworked and can therefore only devote limited attention to important issues. It is hardly surprising, then, that there are still organizations using outdated software and operating systems. This is precisely what makes companies more vulnerable to attack.

The use of AI in IT security solutions saves human resources because the machines make many decisions independently (based on rules), act faster than humans when analyzing, and process significantly more data. political motivated When analyzing log files, algorithms do not overlook anomalies, while humans may have already become tired or no longer look so closely because they want to get off work, for example. AI therefore eliminates the risk of human error.

Why AI-based solutions are essential

Due to the high-risk potential, comprehensive protection for all components of the IT infrastructure is essential. This protection requires seamless monitoring around the clock, which can hardly be achieved by human employees alone. The biggest challenges are limited personnel capacities and the lack of time to recognize the increasingly dynamic and complex attack structures. In addition, the volume of data used to carry out attacks has reached a level that is beyond human control. To counter this problem, companies need to rely on intelligent IT security solutions.

This is precisely where AI-based IT security solutions show their strengths. Not only are they ready for use around the clock, but they can also identify anomalies in large volumes of data almost in real time. Cyberattacks are ultimately deviations from the norm in IT networks that can be detected with the help of AI. In contrast to traditional approaches, some machine learning and deep learning tools do not require predefined rules or information from previous attacks. They learn independently to recognize critical situations. Depending on the solution, log files or real-time analysis of network traffic, for example, serve as the data basis.

Despite the challenges of staff shortages, limited budgets and time pressure, advances in the use of AI in cybersecurity and automation technologies are enabling companies and government organizations to make transformative operational improvements. These technologies significantly accelerate the detection and response to cyber incidents, reduce their cost and impact, and increase cyber resilience.

> *Thanks to the autonomous learning capability of our AI models, we can continuously respond to new threats and constantly improve our security measures."*
>
> **Ziv Grinberg, Vice President Product, Link11**

According to the IBM Institute for Business Value, organizations that rely on these technologies save an average of $3 million on data breaches and reduce the time to respond to cyber incidents by up to 99 days. With a 40% higher return on security investment and significant business growth, AI and automation not only increase cyber resilience but also business value[10].

In the future, companies will have no choice but to rely on AI in IT security if they want to overcome the skills shortage and defend themselves against highly specialized criminals.

Investment in cybersecurity is crucial due to the increasing importance of integrated cyber technology platforms and GenAI. According to PwC's Digital Trust Insights 2024, 84% of German companies want to increase their cybersecurity budget in the future. More and more companies are turning to advanced technologies to mitigate risks and limit financial losses. In Germany, 49% of companies are already using integrated cyber technology platforms (44% globally), and a further 43% (39% globally) plan to make the switch in the next two years.

The use of AI supports security experts in their day-to-day work and helps them to focus on particularly urgent and time-critical tasks without having to compromise on overall security. In Germany, 75% of respondents plan to use GenAI tools for cyber defense in the next 12 months (69% globally)[11]. These figures illustrate the need to invest in modern cybersecurity solutions to effectively counter growing threats.

How Link11 protects you better thanks to AI

Link11 was quick to address the question of how AI can make security solutions even better and thus make companies even more resilient to cyberattacks. Machine learning, pattern recognition, and predictive analytics are becoming integral parts of more and more services.

Bot management: Like AI, bots are not inherently good or bad. The requests generated by these automated programs now account for a large proportion of traffic in many companies. Search engines use bots to index the content of pages. Comparison portals use bots to obtain up-to-date price information. However, bots can also be used fraudulently and criminally. For example, when they retrieve advertising formats with fraudulent intent or restrict the usability of systems in a criminal manner.

With our bot management service, we offer the option of classifying and controlling the traffic caused by bots on your systems. AI helps the system to recognize and assess previously unknown bots. In this way, it helps you use the service to provide real users with a better experience when visiting your sites by reacting to traffic from unwanted bots.

DDoS protection: Link11's cyber resilience network analysis is not the only one to show that DDoS attacks are increasing in number and complexity. Link11's protection solution combines the use of the cloud with AI. Thanks to the cloud, the protection is easily scalable and can be deployed quickly. And with "Always On", the system acts around the clock in the event of an attack, when time plays a crucial role. The AI solution learns in real time from all at-

> *"Our solutions combine technical sophistication with artificial intelligence to deliver tailored responses to our customers' security requirements."*
>
> **Karsten Desler, CTO, Link11**

tacks fended off by Link11. The system analyzes each attack and transfers the results to other threat patterns. Unlike any manual approach, the system is therefore prepared for new attack vectors. This benefits all customers and companies, as the defense shield is constantly improving. It anticipates similar incidents and can therefore react faster in the event of a threat. This automated security not only saves time and money, but also makes it easier for you to concentrate on the essentials.

AI systems do not release us from responsibility

For all its potential, artificial intelligence is not a panacea when it comes to IT security and cyber resilience - at least not for the time being. After intensive training, AI is strong at detecting threats such as malware or DDoS attacks, and is also more accurate than human attack detection in a direct comparison. However, as the threat situation in the digital world is highly dynamic, it will still be up to humans to classify attacks and derive measures from them. The most important tool for this will be AI. It will increasingly take the burden of decision-making off humans but will not replace them completely.

Would you like to find out more about how the use of artificial intelligence can better protect your IT and help you implement your security strategy? Then contact one of our specialists today.

Michael Scheffler
Vice President Sales

+49 69 58004926-306
m.scheffler@link11.com

Sources

1 https://www.mckinsey.de/news/presse/genai-ist-ein-hilfsmittel-um-die-produktivitaet-zu-steigern-und-das-globale-wirtschaftswachstum-anzukurbeln
2 https://www.pwc.de/de/cyber-security/ceosurvey.html
3 https://www.ibm.com/thought-leadership/institute-business-value/report/ai-security-automation
4 https://www.pwc.de/de/cyber-security/digital-trust-insights.html
5 https://www.capterra.com.de/blog/4532/ki-cybersecurity-studie
6 https://www.bitkom.org/Presse/Presseinformation/Organisierte-Kriminalitaet-greift-verstaerkt-deutsche-Wirtschaft-an
7 https://www.accenture.com/us-en/insights/security/state-cybersecurity
8 J. Müller-Quade: Künstliche Intelligenz und IT-Sicherheit. Bestandsaufnahme und Lösungsansätze, April 2019
9 https://www.bitkom.org/Presse/Presseinformation/Rekord-Fachkraeftemangel-Deutschland-IT-Jobs-unbesetzt
10 https://www.ibm.com/thought-leadership/institute-business-value/report/ai-security-automation
11 https://www.pwc.de/de/cyber-security/digital-trust-insights.html

LINK11

Head office

Link11
Lindleystr. 12
60314 Frankfurt