ITW
IT Weapons
A Konica Minolta Division

DEPTH SECURITY
A KONICA MINOLTA SERVICE

GUIDE TO PENETRATION TESTING

Advanced IT help for more protection against constantly emerging cybersecurity threats

PENETRATION TESTING: FOR OPERATIONS PROTECTION FROM ALL DIRECTIONS

Offensive services deliver better defenses to protect enterprise.

The headlines in the media keep coming, and they're scary. Businesses in all types of industries are being attacked by cybercriminals to steal sensitive data, compromise operations and even hold data ransom for big money. In fact, cyberattacks and ransomware are at all-time highs, and continue to grow in their prevalence, complexity and recovery expense.

The fact is, anti-virus security and firewalls simply don't provide enough protection anymore. According to the "Coalition 2023 Cyber Claims Report," the severity of ransomware claims has reached a record high, with the average loss amounting to more than $365,000.[1] And in the U.S., the FBI's Internet Crime Complaint Center reported 2,084 ransomware complaints from January through July of 2021 – a 62 percent year-over-year increase.[2]

The solution to helping organizations try to stay ahead of hackers is through penetration testing, which first involves assessing current levels of security to find and fix any gaps. System vulnerabilities can include code mistakes, software bugs, insecure settings, service configuration errors and/or operational weaknesses. Then, depending on the organization's size and current level of information security requirements, testing can deliberately use cybercriminals' own methods to safely simulate attacks and determine how well the organization's systems and applications can fend them off.

Record-breaking breaches in 2023

According to the Identity Theft Resource Center's 2023 Data Breach Report,[3] the number of reported data breaches jumped 78% in 2023 to their highest total ever. Per the report, there were 3,205 data breaches last, smashing through the prior record of 1,860 set in 2021.

[1] https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

[2] https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

[3] https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/

THE BENEFITS OF PENETRATION TESTING

Pen testing goes well beyond standard security measures.

A penetration test, aka a "pen test," is a special technology assessment that varies by scope and methodology. True pen testing simulates an attack by a malicious party on a network or application to identify flaws in an organization's security, arranged for a specific time and executed with an attempt to avoid damaging any of systems. Following this testing, the pen testing firm will report and describe any issues and weaknesses they found, with suggestions for how to resolve and fortify the weaknesses so that operations are more secure.

Building and maintaining a stronger, more resilient security posture through pen testing can save millions of dollars in downtime and reparation costs – not to mention reputational loss.

Penetration testing benefits businesses by:

- Identifying threats and vulnerabilities that present the most protection risk related to client data, including but not limited to its availability confidentiality and integrity
- Finding vulnerabilities that traditional, control-based testing methodologies often miss
- Uncovering critical and exploitable vulnerabilities in an organization's current technology, people, and processes
- Reducing the risk of ransomware and other emerging threats
- Providing quantitative results that help measure the risk associated with critical assets
- Fulfilling and validating security compliance with critical industry regulations, such as the Payment Card Industry Data Security Standard (PCI DDS) and the Payment Application Data Security Standard (PA-DDS), a global data security standard
- Saving on potential remediation costs and reducing any network downtime
- Developing next-level security measures and solutions for an organization's IT systems
- Protecting a company's reputation and helping to ensure customer loyalty

TODAY'S DRAMATICALLY DIFFERENT WORKPLACE

From endpoint to endpoint and around the world, businesses are at risk.

Business today is global and runs on digital devices and networks – internal, external and mobile – and with growing use of applications and data storage in the cloud, so bad actors have lots of places, potential opportunities and methods to compromise or even shut down a business's operations. Endpoints for desktops, laptops and mobile devices present big security risks because they allow access to central servers and the outside world, and anti-virus software covers a single endpoint and only detects and blocks malicious files.

The new structures and processes of remote work also affect security. Without secure endpoint devices, including often-overlooked printers, and ensuring compliance with secure procedures for accessing data, remote employees can expose their respective companies, partners and vendors to major risks.

While the pandemic seems to be winding down, and companies are bringing employees back into the office, all research points to[4] remote work continuing in a variety of hybrid arrangements. According to two recent studies, findings point to a permanent shift to work from home (WFH) – twice as many workers will be 100 percent remote than before the pandemic, and about 75 percent of the telework increase is likely to be permanent. WFH arrangements has jumped in every major industry, and the rise has been especially sharp among highly educated workers.

First things first: Endpoint security begins inside.

Before moving to penetration testing, it's essential for the head of an organization's IT department to:

- Review and adjust the security settings of the cloud access points in addition to the company's internal network
- Ensure that the security settings and measures for remote users are appropriate for current and foreseeable levels of usage
- Make users and IT staff aware of all the latest security threats to determine if they need more

[4] https://www.bloomberg.com/news/articles/2022-02-28/remote-work-seen-more-persistent-than-u-s-city-planners-expect

PEN TESTING: A CRITICAL STEP TO PROTECT AGAINST CYBERATTACKS

Security measures are often shortchanged due to the speed of business today.

As every industry competes to get ahead in the marketplace, technology development has also been fast-tracked. Mobile apps multiply each year, and more businesses are moving to cloud-native approaches with their technology platforms and other software applications. But it's not always easy (or quick) to integrate security into development and into an organization's current IT infrastructure. It's also easy (and common) for businesses not to keep up with the latest security measures.

The speed at which business moves today means that penetration testing is valuable – and experts would say it's essential – because it can provide insights into an organization's security defenses from a hacker's perspective. With pen testing, businesses can learn about which areas security professionals may have overlooked during applications development, network integration and other areas that can be invisible from the inside.

According to the latest data breach report by[5] IBM and the Ponemon Institute, the average data breach in 2024 among those surveyed cost $4.45 million – a 10% rise and the highest increast since the pandemic. In addition, the average time it took respondents to identify and contain a breach involving stolen credentials was 292 days.

[5] https://www.upguard.com/blog/cost-of-data-breach

WHAT CAN HAPPEN WITHOUT FORTIFIED IT SECURITY

Threat vectors target infrastructure within businesses & countries.

Just prior to Russia's attack on Ukraine, Bloomberg and other news outlets learned that hackers gained access to computers belonging to current and former employees at nearly two dozen major U.S. natural gas suppliers and exporters, including Chevron.[6] And hours before the Russian invasion began on February 24, 2022, Microsoft's Threat Intelligence Center detected a new malware package[7] the company denominated as FoxBlade, which was directed against Ukraine's digital infrastructure. Fortunately, Microsoft provided the Ukrainian government with technical advice to prevent the malware's success.

At about the same time, Goldman Sachs economist Ronnie Walker published a report that highlights research on the potentially extreme threats that malicious cyber criminals could inflict on economies across the globe. Walker's research cites data that cyberattacks cause about $1 trillion in damage to the world economy each year[8]– and two-thirds of those attacks are attributed to Russia. The U.S. has already frequently been threatened and tested by these types of attacks, and experts unanimously agree that there will be more.

Of course, attacks also come from inside the U.S. and many other locations in the world – and even from a bad actor or careless employee inside an organization. It's become essential for businesses to take preventive steps to avoid the potential disruption and expense involved in a data breach or ransom cyberattack of any size.

The oldest privately held trailer manufacturer in the U.S. is still investigating 2021's data breach.[9]

Utility Trailer Manufacturing Company (UTM) is a truck and trailer manufacturing company based out of Los Angeles County, California. Founded in 1914, the company is the largest manufacturer of refrigerated vans and is one of the largest manufacturers of trailers in the United States, with five factories in Utah, Virginia, Alabama and Arkansas.

The company experienced a data security incident in April 2021 when an unauthorized party gained access to files on the company's computer network, which resulted in exposing consumer names, addresses and Social Security numbers. The company sent a breach notification letter to the affected parties, but not until February 2022. Data breach lawyers at Console & Associates, P.C. are still investigating the security breach and interviewing victims. If it turns out that UTC failed to adequately protect consumer data, the affected parties may be able to bring a data breach class action lawsuit against the company.

[6] https://yournews.com/2022/03/11/2312301/hackers-successfully-penetrated-21-u-s-lng-producers-just-before-ukraine/

[7] https://www.zdnet.com/article/microsoft-finds-foxblade-malware-on-ukrainian-systems-removing-rt-from-windows-app-store/

[8] https://www.bloombergquint.com/global-economics/goldman-analyst-warns-cyberwarfare-could-inflict-economic-costs

[9] https://www.jdsupra.com/legalnews/data-breach-alert-utility-trailer-3439853/

MORE EXAMPLES OF RECENT CYBER ATTACKS

Here are some of 2024's biggest data breaches:[10]

UnitedHealth – UnitedHealth was hit with a ransomware attack in April of 2024 that resulted in an enormous $872 million loss and effected an estimated one-third of Americans. Believed to have been executed via a vulnerable Citrix portal, the attack targeted UnitedHealth's ChangeHealthcare payment platform. ChangeHealthcare, which manages transactions between physicians, pharmacies, and healthcare professionals, was suspended after the attackers claimed to have stolen 6 Tb of data.

Cannes Hospital – April was bad month for healthcare data security. On April 16th, healthcare workers at Hospital Simone Veil in Cannes were forced to use pen and paper to handle their job functions after a ransomware attack. The hospital handles 150,000 outpatient appointments and 50,000 emergencies per year.

Trello – In January of 2024, Trello reported that data from 15 million accounts had been leaked. TechRadar reports that "The hacker apparently employed a public API to match an existing database of 50 million emails with Trello accounts… Leaked data – totaling 15,115,516 entries - was offered for sale on a hacking forum, supposedly containing 'emails, usernames, full names and other account info'."

[10] https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021

WHY IT'S SO IMPORTANT TO GUARD AGAINST RANSOMWARE

Education, construction and property, and central and federal government are among the attackers' top 10 industry targets.[11]

According to the Verizon Data Breach Investigations Report, ransomware was involved in 24% of all data breaches, and[12] affected 66% of organizations in 2023.

Since 2020, there have been more than 130 different ransomware strains detected according to VirusTotal's "Ransomware in a Global Context" report.[13]

Clearly, ransomware attacks are growing in number and will be especially damaging threats for years to come. Worse yet is the threat of Ransomware 2.0 that infects cloud software-as-a-service providers. It's important for businesses and organizations of all types to know how these attacks work and to take steps to protect against them.

HOW RANSOMWARE WORKS

As the name implies, ransomware takes an organization's data hostage through encryption, preventing legitimate users from accessing it. It typically goes like this:[14]

13

ACCESS – Most ransomware arrives through phishing emails – messages designed to trick someone into entering their credentials or interacting with malicious content. It could be an Excel file with macros that release ransomware when enabled, a hidden executable file, or a link to a malicious or fake website.

INFECTION – Once released, the virus installs itself on the targeted machine and attempts to gain access to any data, resource or system it can on the organization's network. This includes access keys to the network, important documents or even built-in security measures that could impede the virus' progress.

SPREAD – Ransomware is designed to spread. It infects any machine it can. It will find out as much information as it can about your infrastructure. It will identify and spread to network shares, smart devices and other resources it can access.

ENCRYPTION – Once the virus has spread and gained access to a significant part of an organization's infrastructure, it will "activate" and encrypt all the files it has access to. This is usually the first time an organization's employees realize there's an issue.

DEMAND – After compromising and encrypting, the virus then sends its victims a message making a ransom demand. This could be an ask for payment with a promise to release and return all the files, a warning that sensitive information will be published online, or a threat to sell data on the dark web. In a frightened panic, victims often pay the ransom. Instead of resolving the problem the payment encourages more cybercrime and provides no guarantee that the criminal will release the hijacked data.

[11] https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

[12] https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

[13] https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

[14] Konica Minolta, 2021 – Avoid a Cyber-Hostage Crisis: A Guide to Safeguarding Against Ransomware and Other Emerging Threats in the New Reality of Remote Work

TYPES OF PENETRATION TESTING

Every pen testing engagement is different and depends on the organization's needs.

There are many ways to test an organization's IT systems as well as solutions and technologies to help fill security gaps. Every organization contains a unique combination of architecture, system integrations, sensitive data and users with access. The following are four of the key approaches that can benefit most organizations.

Application Penetration Testing

Web applications and mobile applications are the most vulnerable areas within an organization's environment. The convenient access provided to customers, employees and partners can also serve as the same to potential attackers – so a vulnerable application puts data at risk and allows attackers to pivot and attack the entire internal enterprise.

Network Penetration Testing

More than ever, security leadership and staff are in the position to defend their organization against major global threats, including ransomware attacks, without knowing their complete attack surface. Network penetration testing provides a solid view of an organization's systems and data. This type of penetration testing can be performed in one or any combination of methods: external discovery, external network, internal network, wireless access and trusted access. Pen testing experts can discover gaps in security from a wide variety of threat vectors.

Adversary Emulation

Also called Red Team Testing, this is a real-world test of security controls to prevent a highly skilled adversary from accessing and compromising an organization's data, using the same tools and techniques as attackers. It involves increased timelines and often multiple, concurrent accessors to allow for more advanced tactics, techniques and procedures (TTPS) such as evasion, social engineering (i.e. phishing), physical attacks and the ability to achieve explicitly defined goals.

Security Reviews

While the world moves away from passwords as the sole proof of credentials, password strength is still critical. Modern multifactor authentication (MFA) mechanisms can mitigate some of the external network risks associated with weak user passwords. But internally, MFA is more challenging to deploy in daily use, making password security as relevant as ever – just one weak password can be used by an attacker to compromise the entire enterprise perimeter. Actionable advice on how to strengthen an organization's password environment is essential.

THE DIFFERENCE BETWEEN RED TEAMS AND BLUE TEAMS

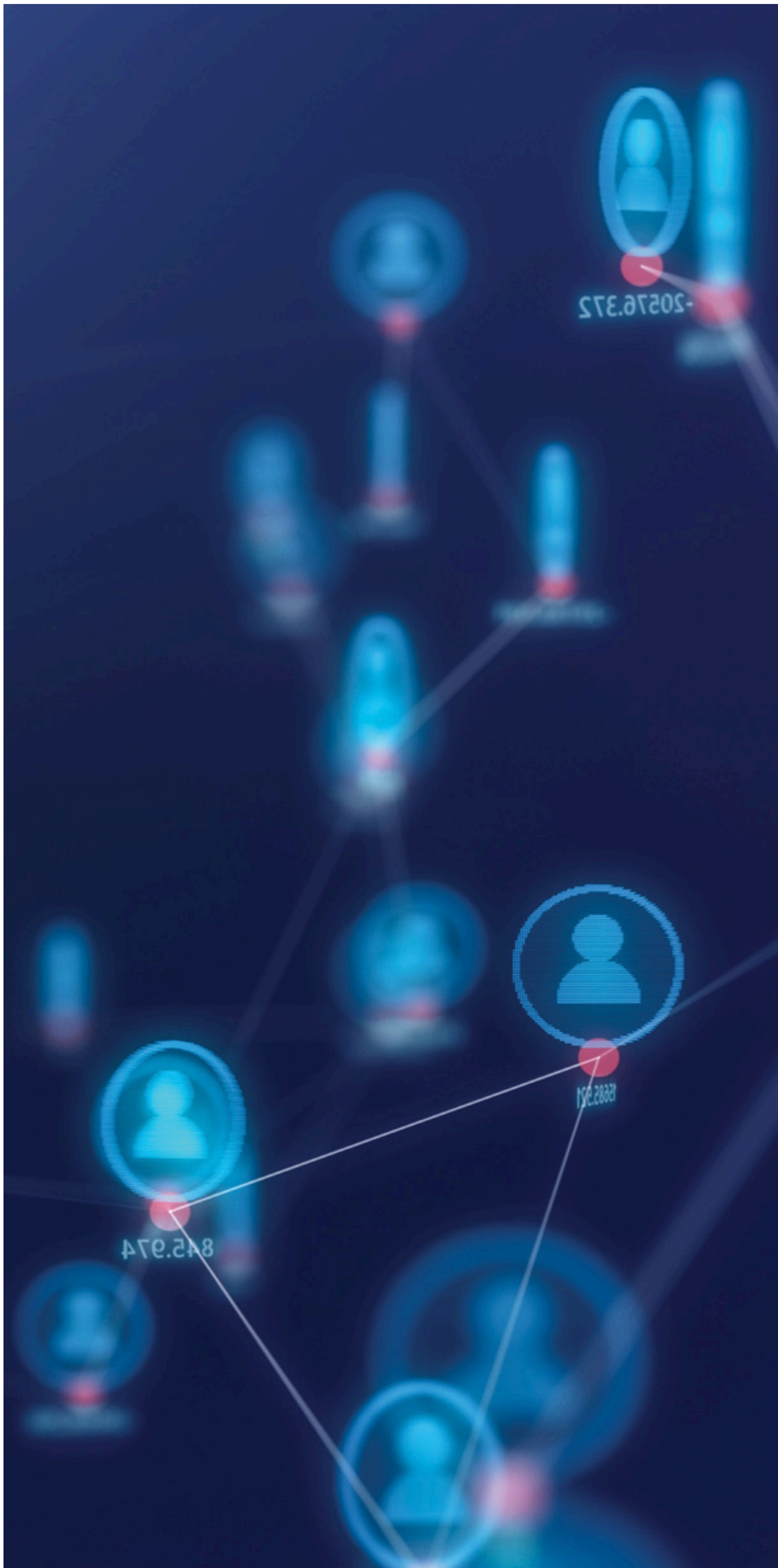
Combining the services of both provides a more complete level of security protection.

While red teams are security engineers who specialize in offensive services to break into security defenses, blue teams are experts in maintaining and defending those internal network controls. The sports analogy is apt – but the activities of each team go well beyond a simulated and competitive "game" to help provide a more up-to-date and fortified security posture.

Red teams are expert and ethical security professionals who objectively evaluate a system's security by using a wide variety of the same techniques cyber criminals use themselves to overcome the security controls within an organization. The red team carefully plans and develops simulated attacks from the outside to test the network's security and discover the organization's weaknesses in people, processes and technologies.

Blue teams, on the other hand, are the security professionals who take an inside-out view of the organization. They learn about the organization's security strategies and key assets by first gathering information about what requires protection. They initially provide a risk assessment, and in the process, may introduce stronger password policies and provide education to staff to make sure everyone understands the necessity of conforming to the organization's security policies and procedures.

But with IT security, the more knowledge, the better – which is why it's best to work with both red and blue teams. When engaging both, management should make sure that the two teams cooperate and keep each other informed and share knowledge and resources in addition to holding regular update meetings with key members of the organization. It's all about continuous security improvements to build a strong and safe IT foundation – because cyber criminals are constantly looking for ways to attack.



DEPTH SECURITY: PENETRATION SERVICES FROM IT WEAPONS

Additional IT expertise through Konica Minolta's Managed IT Services division.

Founded in 2006, Depth Security is a team of highly skilled information security engineers with decades of experience and proven case studies. The team specializes in providing visibility into threats facing infrastructure and operations, with network and application penetration testing and adversary emulation. This is accomplished by creatively simulating real-world attacks using the same tools and techniques as attackers to identify vulnerabilities.

To counter this, the team also designs, builds and deploys next-level information security solutions. These include Network Access Control, Advance Endpoint Protection, Endpoint Application Control, Endpoint Detection and Response, Vulnerability Management, Next Generation Firewall, Next Generation Threat Emulation and Extraction and Mobile Threat Prevention.

The Depth Security team rounds out IT Weapons' current defensive offering to include offensive capabilities. Following the acquisition of VioPoint, IT Weapons' now has both Blue Team (Active Defense security monitoring, Vulnerability Management) and Red Team (Testing Services and Adversary emulation) capabilities, along with best-in-class Managed Security Awareness Training, Threat Landscape and vCISO services.

5 REASONS FOR REGULAR PEN TESTING

- Finds IT system vulnerabilities before the cybercriminals do
- Saves remediation costs and reduces network downtime
- Helps to create stronger defense mechanisms and remediation strategies
- Ensures compliance with leading security standards required by law
- Prevents loss of company reputation and customer loyalty

LEARN MORE ABOUT PENETRATION TESTING TODAY WITH A FREE CONSULTATION FROM DEPTH SECURITY

Depth@kmbs.konicaminolta.us
https://depthsecurity.com
(816) 299-4123

DEPTH
SECURITY
A KONICA MINOLTA SERVICE

About Depth Security
Depth Security is a different type of information security company, founded by a small group of experienced information security engineers and are still run by the same team today. The company culture is deeply anchored in experience, creativity and talent. Unlike many competitors, the people of Depth Security have spent decades in the trenches of IT security, not 50,000 feet up in the clouds. They've been key players at some of the largest IT security organizations and led some of the best corporate information security teams for enterprise organizations. Depth Security has not only designed next- level information security solutions, but the company has also built them and was responsible for them, day to day, in some of the most challenging environments. Most important, the professionals at Depth Security have walked in their customers' shoes – and they understand.

Depth@kmbs.konicaminolta.us
https://depthsecurity.com (816) 299-4123