Security Newsletter

16 December 2019

Subscribe to this newsletter

GDPR: German Privacy Regulator Fines 1&1 Telecom 9.55M EUR for insufficient user verification at Customer Services

On Monday, 1 & 1 Telecommunications was fined €9.55 million ($10.6 million) by Germany's Federal Commissioner for Data Protection and Freedom of Information, or BfDI, for its failure to put in place "sufficient technical and organizational measures" to protect customer data in its call center environments. The company has said it will appeal the fine.

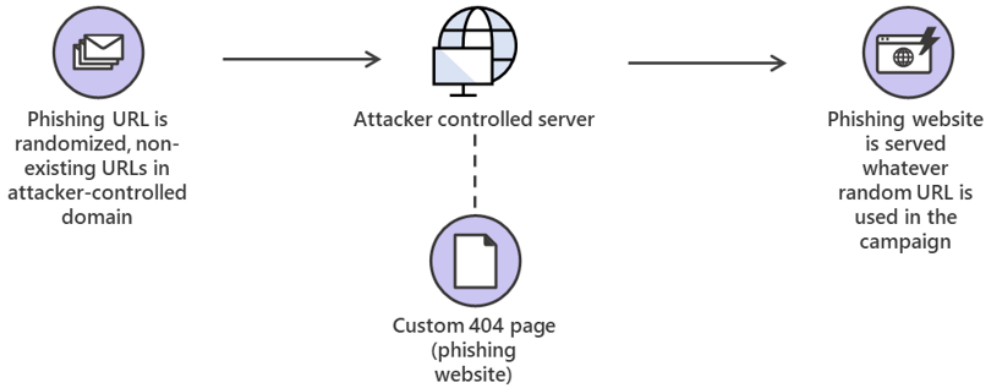
The BfDI says it fined 1 & 1 Telecom after discovering that callers to its call center could retrieve customer information simply by giving their name and date of birth, which it said was an insufficient level of authentication for protecting customer data. "In this authentication procedure, the BfDI sees a violation of Article 32 of GDPR , according to which the company is obliged to take appropriate technical and organizational measures to systematically protect the processing of personal data."

BfDI said that after it "criticized the inadequate data protection, 1 & 1 Telecom GmbH was transparent and very cooperative," adding an extra step to require additional information, which the regulator said was a significant improvement both in terms of the technology applied as well as the resulting data protection improvement. The regulator said it applied a relatively low fine, based on 1 & 1 Telecom's cooperation and move to rapidly fix the problem.

We have had cases on authentication in the past including from a U.K. financial services regulator. Organizations need to check that they are dealing with the right people and that they are not giving data away unnecessarily. When they do spot a possible security vulnerability organizations need to deal with it quickly and efficiently. "Since then, 1 & 1 has continued to evolve its security requirements," the company says. "For example, since then a three-level authentication system has been introduced, and in the next few days 1 & 1 - being one of the first companies in its sector to do so - will provide each customer with a personal service PIN."

Read More on BankInfoSecurity

The quiet evolution of phishing



Earlier this month, Microsoft released a report on this year's malware and cyber-security trends. Among the few trends highlighted in the report was that phishing was one of the few attack vectors that saw a rise in activity over the past two years. Microsoft said that phishing attempts grew from under 0.2% in January 2018 to around 0.6% in October 2019, where 0.6% represented the percentage of phishing emails detected out of the total volume of emails the company analyzed.

Over the years, phishers have become better at evading detection by hiding malicious artifacts behind benign ones. This tactic manifests in, among many others, the use of URLs that point to legitimate but compromised websites or multiple harmless-looking redirectors that eventually lead to phishing. The other way that phishers evade detection is to use multiple URLs and sometimes even multiple domains for their campaigns. They use techniques like subdomain generation algorithms to try and always get ahead of solutions, which, without the right dynamic technologies, will be forced continually catch up as phishers generate more and more domains and URLs. Phishers have also been getting better at impersonation: the more legitimate the phishing emails looked, the better their chances at tricking recipients. Countless brands both big and small have been targets of spoofing by phishers.

Read More at Microsoft Security Blog

Summary on ZDNet

New Plundervolt attack impacts Intel CPUs

A team of cybersecurity researchers demonstrated a novel yet another technique to hijack Intel SGX, a hardware-isolated trusted space on modern Intel CPUs that encrypts extremely sensitive data to shield it from attackers even when a system gets compromised. Dubbed Plundervolt and tracked as CVE-2019-11157, the attack relies on the fact that modern processors allow frequency and voltage to be adjusted when needed, which, according to researchers, can be modified in a controlled way to induce errors in the memory by flipping bits.

"We demonstrate the effectiveness of our attacks by injecting faults into Intel's RSA-CRT and AES-NI implementations running in an SGX enclave, and we reconstruct full cryptographic keys with negligible computational efforts," the researchers said.

"Intel has worked with system vendors to develop a microcode update that mitigates the issue by locking voltage to the default settings," Intel's blog post published today reads. "We are not aware of any of these issues being used in the wild, but as always, we recommend installing security updates as soon as possible."

Read More on ZDNet

Even More on TheHackerNews

More #News

- Your Developers Should be Your SDLC Immune System
- New Zeppelin Ransomware Targeting Tech and Health Companies
- Data leak exposes 750,000 birth certificate applications
- Microsoft Office 365 to Add Message Recall in Exchange Online
- Snatch ransomware pwns security using sneaky 'safe mode' reboot
- Chrome now warns you if your password has been stolen
- Go passwordless to strengthen security and reduce costs
- Google rolls out Verified SMS and Spam Protection in Android
- Threat Intelligence: A Deep Dive
- VISA Warns of Ongoing Cyber Attacks on Gas Pump PoS Systems
- Generated Passwords, UX and Security Absolutism
- Blunt the Effect of the Two-Edged Sword of Vulnerability Disclosures

#Patch Time!

- Patch Tuesday, December 2019 Edition
- The december 2019 security update review by ZDI
- OpenBSD patches authentication bypass, privilege escalation vulnerabilities
- Qualys advisory on the OpenBSD vulnerability
- Adobe patches 17 critical code execution bugs in Photoshop, Reader, Brackets
- NVIDIA Patches High Severity Flaws in Tegra Linux Driver Package
- Vulnerabilities Found in Aviatrix Enterprise VPN
- Weidmueller Patches Critical Vulnerabilities in Industrial Switches
- VMware Patches ESXi RCE Vulnerability That Earned Hacker $200,000
- Apple Patches Over 50 Vulnerabilities in macOS Catalina
- Chrome 79 Patches Critical Vulnerabilities

#Tech and #Tools

- MacOS Filename Homoglyphs Revisited
- Cracking LUKS/dm-crypt passphrases
- batea: AI-based, context-driven network device ranking
- Introduction to router exploit kits
- Cloud Network Security 101: AWS Security Groups vs NACLs
- Mind your Logs : How a build log from a Jenkins leaked everything
- How Auth0 Automates Phishing Response
- Windows 10 UAC bypass for all executable files which are autoelevate true .
- MacOS red team: calling apple apis without building binaries
- wpbrute-rs: High perf Wordpress bruteforcer

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. You can find all our open vacancies on our career page.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us