[公开]360BEST-DST-0-010-20200907

大数据协同安全技术
国家工程实验室
National Engineering Laboratory for Big Data Collaborative Security Technology

全球数据安全观察

总第 10 期 2020 年第 10 期

（2020.9.07-2020.9.13）

大数据协同安全技术国家工程实验室

全球动态

1、阿根廷的官方移民局网络系统遭受 Netwalker 勒索软件攻击，被迫停止 4 小时服务

2020 年 9 月 7 日报道，阿根廷的官方移民局 DirecciónNacional de Migraciones 遭受了 Netwalker 勒索软件攻击，该攻击暂时阻止了过境进出该国。尽管针对城市和地方机构的勒索软件攻击已变得司空见惯，但这可能是对已中断一个国家运营的联邦机构的首次已知攻击。

https://www.bleepingcomputer.com/news/security/ransomware-attack-halts-argentinian-border-crossing-for-four-hours/

2、属于 Digital Point 网站管理员论坛的数据库泄漏了超过 80 万用户的记录

2020 年 9 月 7 日，WebsitePlanet 研究小组和网络安全研究员 Jeremiah Fowler 发现了一个不安全的 Elasticsearch 数据库，其中包含超过 6200 万条记录。泄漏中总共包括了 863,412 个 Digital Point 用户的数据。

https://www.zdnet.com/article/webmaster-forum-database-exposed-data-of-800000-users/

3、黑客窃取了澳大利亚政府机构的 738 GB 数据

2020 年 9 月 7 日，新南威尔士州服务局透露，网络攻击导致 47 个员工电子邮件帐户遭到入侵。结果，黑客窃取了大约 186,000 个客户的个人详细信息，这些数据总计 738GB，包含 380 万份文档。

https://www.hackread.com/hackers-stole-738-gb-data-australian-government-agency/

4、中方提出《全球数据安全倡议》

2020 年 9 月 8 日上午，国务委员兼外长王毅在“抓住数字机遇，共谋合作发展”国际研讨会高级别会议上发表题为《坚守多边主义 倡导公平正义 携手合作共赢》的主旨讲话，提出《全球数据安全倡议》。王毅表示，有效应对数据安全风险挑战，应遵循三原则：

(1) 秉持多边主义

(2) 兼顾安全发展

(3) 坚守公平正义

https://www.fmprc.gov.cn/web/wjbzhd/t1812943.shtml

5、斯洛伐克加密货币交易所 ETERBASE 泄露 540 万美元

2020 年 9 月 10 日，总部位于布拉迪斯拉发的加密货币

交易所 ETERBASE 披露了一项安全漏洞。该交易所表示，黑客破坏了其内部网络并偷走了价值 540 万美元的加密货币资金。

https://securityaffairs.co/wordpress/108085/digital-id/eterbase-hacked.html

6、智利银行遭到勒索软件攻击导致所有分行被迫关闭

2020 年 9 月 9 日报道，智利三大银行的国家银行（BancoEstado)的所有分行在 9 月 7 日周一仍处于关闭状态，可能还要停业多日。据消息人士称，该银行的内部网络感染上了 REvil（Sodinokibi）勒索软件。

https://www.secrss.com/articles/25424

7、Netwalker 勒索软件袭击了巴基斯坦主要的电力供应商 K-Electric

2020 年 9 月 9 日报道，巴基斯坦卡拉奇市的电力提供商 K-Electric 受 Netwalker 勒索软件攻击的打击，该攻击阻止了计费和在线服务。Netwalker 勒索软件运营商要求支付价值 385 万美元的比特币。和往常一样，如果公司在七天内不支付赎金，赎金将增加到 770 万美元。

https://securityaffairs.co/wordpress/108075/malware/k-electric-n

etwalker-ransomware-attack.html

8、Secureworks 收购漏洞管理平台 Delve

2020 年 9 月 10 日报道，Secureworks 已收购 Delve，以将新的漏洞管理解决方案引入该公司的产品组合。该公司开发的技术也将集成到 Secureworks 的 Red Cloak 和 TDR 威胁检测平台和应用程序中。此项收购预计将在 2020 年第三季度完成，尚待监管部门批准。

https://www.zdnet.com/article/secureworks-acquires-vulnerability-management-platform-delve/

9、南澳大利亚大学表示区块链与隐私条例不符

2020 年 9 月 10 日报道，南澳大利亚大学（UniSA）表示当前区块链平台存在固有的关键隐私问题。这是由于区块链使用先前交易的详细信息来嵌入数据链来验证未来交易，并且系统的生存能力还取决于每个区块的不可编辑性。UniSA 新兴技术研究员 Wahlstrom 指出了诸如欧洲通用数据保护条例（GDPR）之类的法律中存在“被遗忘的权利”，他说区块链的内在思想与该条例相冲突。

https://www.zdnet.com/article/university-of-south-australia-says-blockchain-at-odds-with-privacy-obligations/

10、塞舌尔银行遭到勒索软件攻击

2020 年 9 月 12 日，塞舌尔中央银行（CBS）在一份新闻声明中透露，塞舌尔发展银行（DBS）遭到勒索软件攻击。根据新闻稿，勒索软件攻击于 2020 年 9 月 9 日发生。CBS 和 DBS 立即对事件进行了调查，并正在评估攻击的程度。

https://securityaffairs.co/wordpress/108199/cyber-crime/bank-of-seychelles-ransomware-attack.html

11、Razer 数据泄漏暴露了游戏玩家的个人信息

2020 年 9 月 12 日报道，游戏硬件制造商 Razer 在其在线商店的不安全数据库被在线暴露后遭受了数据泄漏。该数据库被错误地配置为可供公众访问，暴露了大约 100,000 个从 Razer 在线商店购买商品的用户个人信息。暴露的信息包括客户的姓名，电子邮件地址，电话号码，订单号，订单明细以及帐单和送货地址。

https://www.bleepingcomputer.com/news/security/razer-data-leak-exposes-personal-information-of-gamers/

12、泄漏的服务器暴露了数十万约会网站用户的个人详细信息

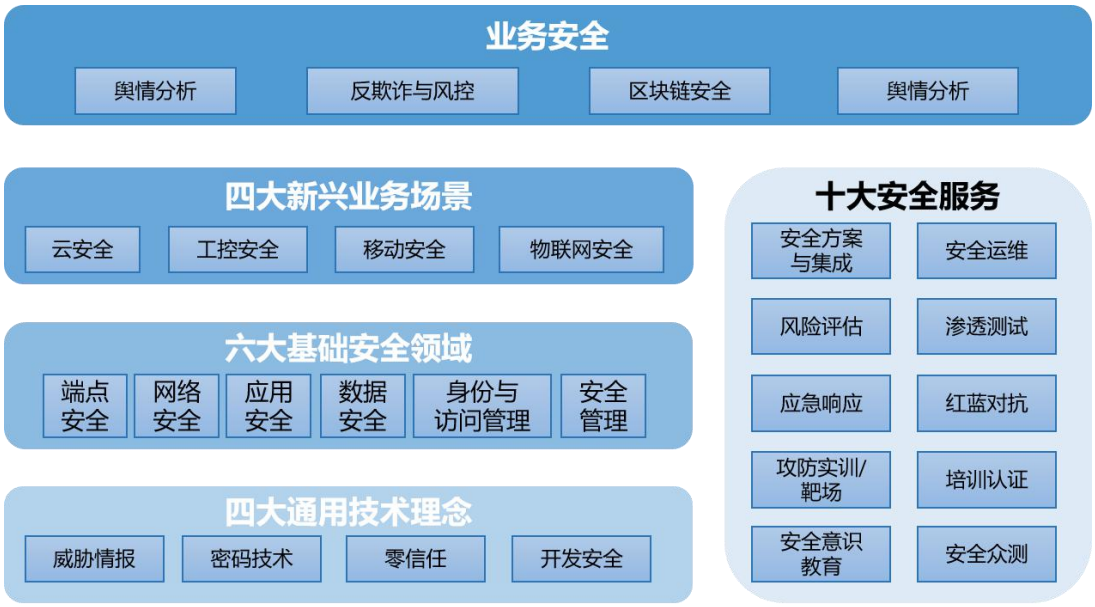
2020 年 9 月 13 日报道，一个没有密码就暴露在网上的在线数据库泄露了成千上万注册在线约会网站的用户的个人详细信息。vpnMentor 的安全研究人员于 8 月底发现了泄漏的数据库，该数据库存储了超过 882 GB 的日志文件，总共包含过去 96 个小时内发送的 6600 万条个人通知的详细信息，以及数十万用户的个人详细信息。

https://www.zdnet.com/article/leaky-server-exposes-users-of-dating-site-network/

业界观点

1、2020 年中国网络安全市场全景图，其中数据安全属于六大基础安全领域之一

如图所示，本次全景图发布六大基础安全领域、四大通用技术理念、四大新兴应用场景、业务安全和安全服务，共计 16 类一级安全板块、78 类二级细分领域。分类主要参考了国家质量监督检验检疫总局、国家标准化管理委员会发布的 23 项国家标准和公安部发布的 26 项行业标准。



https://www.secrss.com/articles/25335

2、几乎所有网络安全公司都在泄露敏感数据

根据 ImmuniWeb 的一项新研究，几乎所有网络安全公司都在线暴露了包括 PII（个人隐私信息）和密码在内的敏

感数据。**员工安全意识薄弱是造成这种糟糕局面的主要原因。**报告声称，已发现经过验证的（来自网络安全公司的）敏感数据泄露事件超过 63.1 万次，其中这些“事件”中有 17%具有重大风险。这意味着泄露数据包括使用纯文本密码的登录名，或者包括最近和/或唯一的数据泄漏（例如 PII 和财务记录）。

https://www.aqniu.com/threat-alert/70069.html

3、数据安全治理的九大要素

数据安全治理是围绕着风险，针对面临的各种风险，制定针对性的策略，将风险减少至可以接受的程度。数据安全治理的九大要素包括：安全目标与业务目标对齐、梳理数据资产、识别敏感数据、数据认责体系、分类分级策略、访问控制策略、安全审计策略、组织与人员、制度与流程、技术与工具。

https://www.secrss.com/articles/25340

4、《2020 年中国网络安全十大创新方向》报告发布

(1) 网络空间测绘

(2) SOAR 安全编排自动化与响应

(3) 密码技术

(4) 欺骗技术

(5) 开发安全

(6) 数据安全治理

(7) 身份与访问管理

(8) 终端监测与响应

(9) 软件定义边界

(10) 网络监测与响应

https://www.secrss.com/articles/25521

5、2020 年勒索软件攻击最多的四大漏洞

报告显示，勒索软件是 2020 年最猖獗的，同时也是给企业造成损失最大的攻击手段。根据 SenseCy 的最新研究，勒索软件攻击并不都是由 Windows 漏洞触发的，很多攻击者利用了用于远程访问 Windows 网络的工具中的漏洞。以下是研究人员发现的**勒索软件热衷使用的四大漏洞：**

(1) CVE-2019-19781：Citrix 应用程序交付控制器

(2) CVE-2019-11510：Pulse VPN 漏洞

(3) CVE 2012-0158：微软 Office 通用控件

(4) CVE-2018-8453：Windows Win32k 组件

因此，勒索软件全面防护，始于漏洞管理。

https://www.secrss.com/articles/25472

6、《贯彻落实网络安全等保制度和关保制度的指导意见》解读与信号释放

9 月 2 日，2020 年 9 月 2 日，由公安部网络安全保卫局指导，公安部第三研究所、公安部第一研究所主办的“网络安全等级保护和关键信息基础设施安全保护工作宣贯会”在京召开。其中有强调**要落实密码安全防护要求**。应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。

https://www.freebuf.com/articles/neopoints/249161.html

7、构成“零信任生态系统”的 7 个主要元素

企业的业务和商业流程已不再局限于物理环境内，传统以网络边界为中心的防火墙式安全防护机制已无法满足企业的发展要求，企业需要转向构建一个以数据和身份为中心的、与当下数字化发展趋势更加相适应的安全防护机制。因此，从 2018 年开始，Forrester 开始发布零信任拓展生态系统 Zero Trust eXtended (ZTX) 研究报告，并提出 7 个构成 ZTX 生态系统的主要元素。

(1) 网络安全能力

(2) 数据安全

(3) 身份安全

(4) 工作负载/应用安全

(5) 设备安全

(6) 可视化与分析

(7) 自动化和编排

https://www.freebuf.com/articles/security-management/247803.html

8、2020 年上半年，勒索软件占所有网络保险索赔的 41%

根据北美最大的网络保险服务提供商之一 Coalition 在 2020 年 9 月 10 日发布的报告显示，勒索软件事件已占 2020 年上半年提交的网络保险索赔的 41%，每次安全事件的网络保险索赔额从 1,000 美元到超过 200 万美元不等。其中，迷宫勒索软件组织最为贪婪，该组织要求勒索赎金的要求是整体平均水平的六倍。

https://www.zdnet.com/article/ransomware-accounts-to-41-of-all-cyber-insurance-claims/