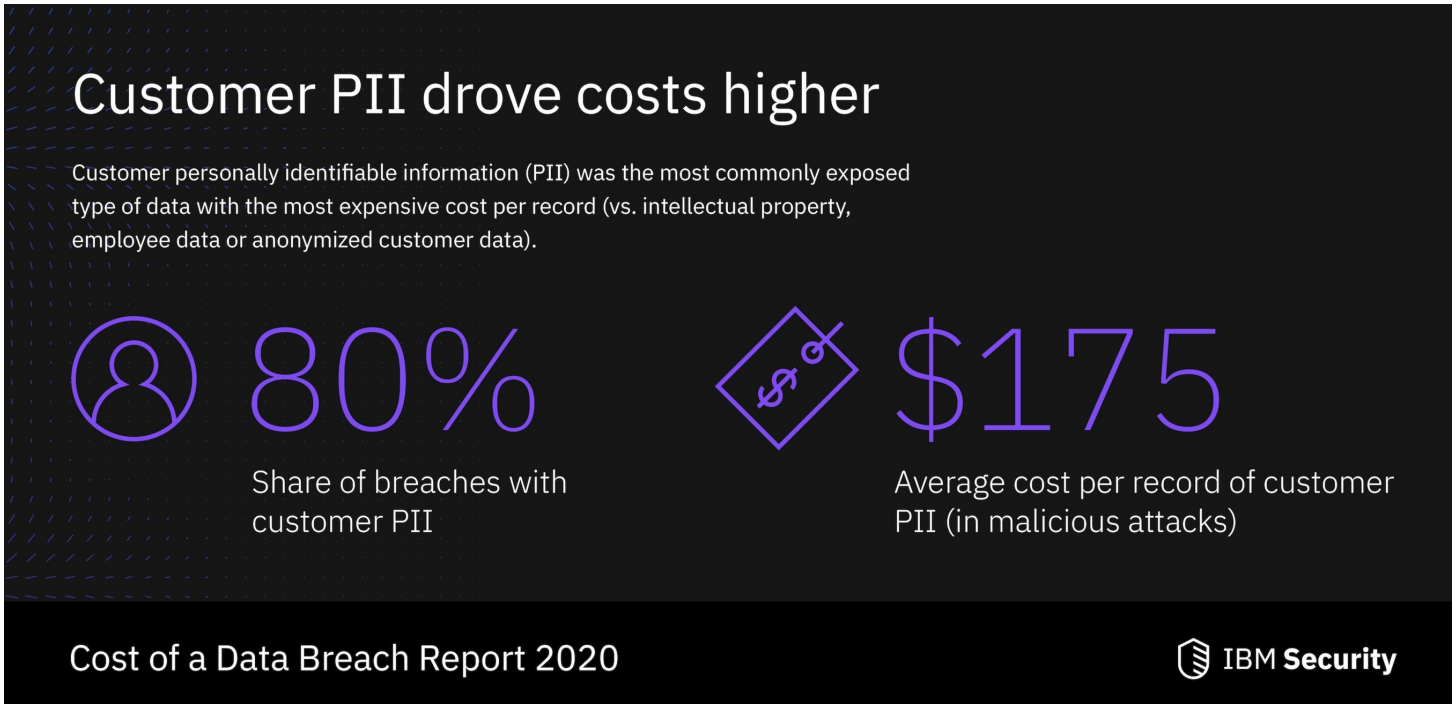
IBM Hong Kong newsroom

IBM 《2020年數據洩露成本報告》 過去一年中成本最高的數據洩露事件源自員工 遭受攻

80%數據洩露事件導致客 個人數據暴露 人工智能和自動化能 顯著降低成本



2020年 8月10日 -- IBM Security 發 《2020年數據洩露成本報告》 宣 其全球調 結果。該項調 研究了數據洩露的財務影響 示了數據洩露事件給企業造成的平均成本為 386萬美元 而其中員工 遭受攻 是最昂貴的原因。對全球 500多個組織數據洩露事件的深入分析發現 有 80%的事件導致了客 個人可識別訊息 (PII Personally Identifiable Information) 暴露。在因數據洩露而暴露的所有數據類型中 客 PII 也是造成企業耗費成本最高的一項。

企業越來越多地通過新的遙距工作模式、 基於雲的業務運營模式來訪問敏感數據 為此 該報告還闡明這些數據遭受洩露後組織可能遭受的財務損失。IBM 的 一項調 發現 儘管這種工作方式轉變已經引起了風險模型的變化 但超過半數的因新冠疫情而開始居家 公的員工並未獲得有關如何處理客 PII 的新準則。

《2020 年數據洩露成本報告》是由 IBM Security 贊助、Ponemon Institute 編寫 基於過去一年中遭受數據洩露的組織中的 3,200 多名安全專業人員的深入訪談而編製。1

今年報告的一些重要調 結果包括

- 智能技術將數據洩露成本降低了一半 與尚未部署安全自動化技術的公司相比 已完全部署了此類技術的公司 即利用 AI、分析和自動編排來識別和響應安全事件的公司 所遭受的數據洩露成本要減少一半 245萬美元對 603萬美元 。
- 為受攻 的憑證「買單」 在攻 者利用被盜或受到攻 的憑證訪問公司網絡而導致的事件中 公司遭受的數據洩露成本比全球平均水平高出近 100萬美元 – 次數據洩露的成本高達 477萬美元。利用第三方漏洞是造成惡意數據洩露成本第二高的根本原因 高達 450萬美元 。
- 特大型數據洩露事件的成本飆升數百萬美元2 超過 5,000萬條記 被洩露的數據洩露事件的成本 從去年的 3.88億美元躍升至

3.92億美元。洩露記 條數從 40到 5000萬條不等的數據洩露事件的平均成本達到 3.64億美元 與 2019年相比 該項成本 加了 1,900萬美元。

- 民族國家攻 – 最具破壞性的數據洩露 據報告研究 相對於其它攻 者而言 始於民族國家的攻 導致的數據洩露事件成本最高。由國家資助的攻 造成的數據洩露事件平均成本為 443萬美元 高於出於經濟動機的網絡犯罪分子和 客造成的數據洩露事件成本。

IBM X-Force 威脅情報副總裁 Wendi Whitmore 表示 「在企業減緩數據洩露影響的能力方面 我們看到部署了自動化技術的公司擁有明顯的優勢。隨著企業以更快的速度擴展其數位化業務 加上安全行業的人才短缺情況持續存在 團隊因需要保護更多的設備、系統和數據而不堪重負。安全自動化可以解決這一負擔 不僅可以實現更快的洩露響應 而且還可以顯著提高成本效益。」

員工憑證及雲配置錯誤¬ – 攻 者選擇的切入點

報告顯示 憑證被盜或受攻 以及雲配置錯誤是導致惡意數據洩露事件的最常見原因 比近 40%。2019年共有超過 85億項記 被暴露在五分之一的所分析數據洩露事件中 攻 者使用了先前暴露的電子郵件和密碼 因此 企業已經開始通過採用零信任的方法來重新考慮其安全策略 – 重新審視他們在用 身 驗證方面的方式和程度。

同樣 公司在應對安全性複雜性 數據洩露成本的主要因素之一 方面遭遇的困境也使得雲配置錯誤成為日益嚴峻的安全性挑戰之一。2020年的報告顯示 攻 者有幾乎 20%的時間選擇通過雲配置錯誤來破壞網絡 這導致數據洩露成本平均 加了 50多萬美元 達到了 441萬美元 使得雲配置錯誤成為了報告中成本第三高的初始感染媒介。

國家資助的攻 所造成的危害最大

2020年的報告顯示 儘管由國家資助的威脅攻 者造成的數據洩露事件在惡意事件中的 比只有 13% 但此類卻是最具破壞性的事件 這表明出於經濟動機的攻 比為 53% 不會為企業帶來更高的財務損失。由國家支持的攻 具有高度戰術性、長期性和隱蔽性等特點 而且針對的都是高價 數據 因此通常會導致受害者環境受到更大範圍的破壞 導致平均數據洩露成本 加至 443萬美元。

實際上 與其他地區相比 中東 來是由國家發起的攻 活動 比比較高的地區 其數據洩露平均成本 年 長 9% 在受調 的 17個地區中是數據洩露平均成本第二高的地區 高達 652萬美元 。 同樣 能源行業也是最經常被民族國家攻 所針對的領域之一 其數據洩露成本同比 長了 14% 平均達到 639萬美元。

高級安全技術有助於提升業務智能水平

該報告強調了實施高級安全技術的企業與落後企業之間的數據洩露成本鴻溝越來越大 具體來 完全部署了安全自動化技術的公司與尚未部署此類技術的公司相比 節省了 358萬美元的成本。兩者之間的成本差距從 2018年的 155萬美元 加到了 200萬美元。

通過完全部署安全自動化技術 企業響應數據洩露所需的時間大幅縮短 這是降低數據洩露成本的一個關鍵因素。該報告顯示 人工智能、機器學習、分析和其他形式的安全自動化技術使得完全部署了安全自動化技術的公司對數據洩露的響應速度比尚未部署安全自動化的公司要快 27%以上 後者平均需要多出 74天才能識別並遏制數據洩露。

事件響應 (IR) 方面的準備程度也繼續嚴重影響著數據洩露的財務後果。既沒有成立 IR 團隊也沒有制定 IR 計劃測試的公司 其數據洩露平均成本為 529萬美元 而成立了 IR 團隊並使用 面演練或模擬來測試 IR 計劃的公司 其數據洩露平均成本則比前者低 200萬美元 這再次表明瞭充分的準備可在網絡安全方面 生可觀的投資回報。

今年報告還披露了一些其他調 結果

- 遙距工作風險將會招致成本 – 該報告顯示 由於混合工作模式導致工作環境受控程度較低 因此在新冠疫情期間採用遙距 公模式的公司中 70%的公司預計將會 加數據洩露的成本。
- 儘管決策權有限 但首席訊息安全主管仍然要為數據洩露負責 儘管只有 27%的受訪者表示 CISO/CSO 是其所在組織的安全策

略和技術決策者 但 46%的受訪者表示 他們的 CISO/CSO 最終都要對數據洩露事件負責 該報告顯示 相比單次數據洩露的平均成本 任命 CISO 可以 助企業節省 14.5萬美元的成本。

- 大多數購買網絡保險的企業都使用索賠來支付第三方費用 該報告顯示 購買了網絡保險的組織的數據洩露平均成本比全球平均 386萬美元要低近 20萬美元。實際上 在購買了網絡保險的組織中 有 51%的組織將索賠用於支付第三方咨詢費和律師費 而 36%的組織將其用於受害者的賠償。只有 10%的受訪者表示會支付勒索軟件的費用或勒索費用。
- 區域和行業洞察力 儘管美國企業的數據洩露成本仍然居於全球首位 平均達到 864萬美元 但報告顯示 斯堪的納維亞地區的數據洩露成本同比 幅最大 接近 13%。醫療保健行業仍舊是數據洩露平均成本最高的行業 高達 713萬美元 – 與 2019年相比 幅超過了 10%。

IBM 《2020年數據洩露成本報告》分享地址
中文 www.ibm.com/account/reg/cn-zh/signup?formid=urx-46693
英文 www.ibm.com/security/digital-assets/cost-data-breach-report/

關於本次調
本年度數據洩露成本報告基於對 2019年 8月至 2020年 4月發生的真實數據洩露事件的深入分析而編製 同時考慮了數百個成本因素 包括法律、法規和技術活動以及品牌資 損失、 客 和員工生 效率損害等。

歡迎註冊參加將於 2020年 8月 12日 星期三 上午 11:00 美國東部時間 舉行的「2020年數據洩露成本報告網絡研討會」 ibm.biz/BdqhMf

關於 IBM Security
IBM Security 可以提供最先進、集成的企業安全 品和服務組合。由世界著名的 IBM X-Force® 研究進行支持 該組合使企業能有效地管理風險並防範新威脅。IBM 作為世界上覆蓋範圍最廣的安全研究、開發和交付企業之一 天對 130多個國家/地區的 700億次安全事件進行監控 並在全球範圍 擁有 10,000多項安全專利。有關更多訊息 請登 www.ibm.com/security 在推特上關注 IBMSecurity 或瀏覽 IBM Security Intelligence 博客。

1該報告分析了 2019年 8月至 2020年 4月之間發生的數據洩露事件。關於採用分析方法的局限性 報告中亦有闡述。
2《2020 年數據洩露成本報告》基於對特定樣本的單獨分析 研究了特大型數據洩露事件 即 失或被盜記 條數超過 100萬條的數據洩露事件 的成本。
3IBM 2020 X-Force 威脅情報指數報告顯示 https://ibm.biz/downloadxforcethreatindex

---

https://hongkong.newsroom.ibm.com/news-releases?item=122399