

2012 DATA BREACH INVESTIGATIONS REPORT

Eine vom Verizon RISK-Team durchgeführte Studie in Zusammenarbeit mit der australischen Bundespolizei, der niederländischen High Tech Crime Unit, dem irischen Reporting & Information Security Service, der Police Central e-Crime Unit der London Metropolitan Police und dem United States Secret Service



2012 DBIR: EXECUTIVE SUMMARY

2011 wird mit großer Wahrscheinlichkeit als ein Jahr der gesellschaftlichen und kulturellen Aufstände in die Geschichte eingehen. Bürger begehrten gegen ihre Regierungen auf, forderten sie heraus oder stürzten sie sogar in einem Dominoeffekt, der seither unter dem Begriff „arabischer Frühling“ geläufig ist, obwohl er länger als eine einzige Saison dauerte. Diejenigen, die sich darüber empörten, was sie als das „eine Prozent“ der geldgierigen Reichen verstehen, besetzten die Wallstreet und andere Städte und Orte überall auf der Welt. An Beispielen hierfür herrscht kein Mangel.

Dieser Zustand allgemeiner Unruhe, der so charakteristisch für das Jahr 2011 war, beschränkte sich jedoch nicht nur auf die physische Welt. Die Online-Welt war ebenso geprägt von aufeinander prallenden Idealen, die sich in Form von Aktivismus, Protesten, Vergeltungsaktionen und Schabernack manifestierten. Obwohl diese Aktivitäten mehr als Datenverletzungen (z. B. DDoS-Angriffe) umfassten, war der Diebstahl von Firmen- und persönlichen Informationen sicherlich eine Kerntaktik. Dieses in neuer Gestalt wieder zum Leben erweckte Gespenst des „Hacktivismus“ geistert nun durch Unternehmen auf der ganzen Welt. Viele, die von der zwielichtigen Natur seiner Herkunft und seinem Hang dazu, seine Opfer in eine peinliche Lage zu bringen, beunruhigt sind, fanden diesen Trend beängstigender als andere Bedrohungen, seien sie real oder imaginär. Doppelt besorgniserregend war für viele Unternehmen und Führungskräfte, dass die Auswahl der Ziele durch diese Gruppen nicht den logisch nachvollziehbaren Kriterien folgte, ob jemand Geld und/oder wertvolle Informationen besitzt. Feinde werden noch bedrohlicher, wenn man ihr Verhalten nicht vorhersagen kann.

Dieses in neuer Gestalt wieder zum Leben erweckte Gespenst des „Hacktivismus“ geistert nun durch Unternehmen auf der ganzen Welt.

Aber es herrschten nicht nur Protest und Schadenfreude. Professionelle Cyberkriminelle automatisierten und optimierten weiterhin ihre bevorzugte Methode der risikoarmen Massenangriffe auf schwächere Ziele. Weit weniger häufig, dafür aber wohl schädlicher, waren fortgesetzte Angriffe auf Geschäftsgeheimnisse, vertrauliche Informationen und anderes geistiges Eigentum. Wir sind im vergangenen Jahr natürlich vielen Ausprägungen, mannigfaltigen Taktiken und unterschiedlichen Motiven begegnet, und in vieler Hinsicht ist der 2012 Data Breach Investigations Report (DBIR) ein Bericht über die vielfältigen Facetten des Datendiebstahls in Unternehmen.

855 Verstöße, 174 Millionen kompromittierte Datensätze

In diesem Jahr werden in unserem DBIR mehr Vorfälle berücksichtigt, die von mehr Mitwirkenden beigesteuert wurden, und er repräsentiert einen breiteren und stärker diversifizierten geographischen Bereich. Die Zahl der kompromittierten Datensätze aus diesen Vorfällen schoss in eine Höhe von bis zu 174 Millionen, nachdem sie einen Tiefststand (oder

Diese Organisationen haben maßgeblich zu einer Verbreiterung des Spektrums des DBIR in Bezug auf Datenverletzungen überall auf der Welt beigetragen. Wir danken ihnen allen sehr für ihren Kooperationsgeist und hoffen aufrichtig, dass dieser Report einen Beitrag dazu leistet, dass das Bewusstsein für Cyberkriminalität wächst und wir künftig gemeinsam besser in der Lage sind, sie noch effektiver zu bekämpfen.

Höchststand, je nach Betrachtungsweise) von 4 Millionen im Vorjahresbericht erreicht hatte. In der Tat verzeichneten wir im Jahr 2011 den zweithöchsten Datenverlust seit Beginn unserer Untersuchungen im Jahr 2004.

Wie schon im vergangenen Jahr, freuen wir uns, dass der United States Secret Service (USSS) und die niederländische High Tech Crime Unit (NHTCU) sich erneut am diesjährigen Bericht beteiligt haben. Wir begrüßen darüber hinaus die australische Bundespolizei (AFP), den irischen Reporting & Information Security Service (IRISS) sowie die Police Central eCrimes Unit (PCeU) der London Metropolitan Police in unserem Team. Diese Organisationen haben maßgeblich zu einer Verbreiterung des Spektrums des DBIR in Bezug auf Datenverletzungen überall auf der Welt beigetragen. Wir danken ihnen allen sehr für ihren Kooperationsgeist und hoffen aufrichtig, dass dieser Report einen Beitrag dazu leistet, dass das Bewusstsein für Cyberkriminalität wächst und wir künftig gemeinsam besser in der Lage sind, sie noch effektiver zu bekämpfen.

Einschließlich der bei Verizon im Jahr 2011 registrierten Fälle und der Daten, die von den oben genannten Organisationen beigesteuert wurden, umfasst die DBIR-Reihe nunmehr acht Jahre, über 2.000 Datenverletzungen und mehr als eine Milliarde kompromittierte Daten. Es war eine faszinierende und lehrreiche Reise, und wir sind all jenen dankbar, die uns auf diesem Weg begleitet haben. Wie immer besteht unser Ziel darin, unsere Leser mithilfe der Daten und Analysen in diesem Bericht bei der Planung von Sicherheitsmaßnahmen zu unterstützen. Nachfolgend zunächst einige Highlights:

DATENERFASSUNG

Die zugrunde liegende, von Verizon angewandte Methode hat sich im Vergleich zur Vorgehensweise in den zurückliegenden Jahren nicht verändert. Sämtliche Ergebnisse beruhen auf Nachweisen aus erster Hand, die in von Verizon in den Jahren 2004 bis 2011 im Kundenauftrag durchgeführten externen forensischen Untersuchungen gesammelt wurden. USSS, NHTCU, AFP, IRISS und PCeU unterscheiden sich in der genauen Methode zur Erhebung der Daten, die sie zu diesem Bericht beigetragen haben, aber sie verfolgen grundsätzlich denselben Ansatz. Alle nutzten VERIS als gemeinsamen Nenner, verwendeten jedoch unterschiedliche Mechanismen bei der Dateneingabe. Aus den zahlreichen Untersuchungen, die von diesen Organisationen im Jahr 2011 geführt wurden, wurden gemäß dem Schwerpunkt des DBIR lediglich die Fälle übernommen, die bestätigte organisationsbezogene Datenverletzungen betrafen.

EINE KURZE EINFÜHRUNG IN VERIS

VERIS ist ein Rahmenwerk, das entwickelt wurde, um eine gemeinsame Sprache für die Beschreibung von Sicherheitsvorfällen strukturiert und wiederholbar zur Verfügung zu stellen. Es übersetzt die Frage „Wer hat was, wem, mit welchem Ergebnis angetan?“ in die Art von Daten, die in diesem Bericht dargestellt sind. Da viele Leser Fragen zu der dem DBIR zugrunde liegenden Methode gestellt haben und weil wir hoffen, den Austausch von Informationen über Sicherheitsvorfälle dadurch vereinfachen zu können, haben wir VERIS für die kostenlose öffentliche Nutzung freigegeben. Einen kurzen Überblick über VERIS finden Sie auf unserer [Website](#)¹, und das vollständige Rahmenwerk ist im [VERIS community wiki](#) erhältlich.² Beides sind gute Begleitreferenzen für diesen Bericht, um die Terminologie und den Kontext besser verstehen zu können.

¹ http://www.verizonbusiness.com/resources/whitepapers/wp_verizon-incident-sharing-metrics-framework_en_xg.pdf

² <https://verisframework.wiki.zoho.com/>

ZUSAMMENFASSENDE STATISTIKEN

WER STECKT HINTER DATENSICHERHEITSVERLETZUNGEN?

98% hatten externe Ursachen (+6 %)

4% wurden von Insidern begangen (-13 %)

<1% wurden von Geschäftspartnern verursacht (↔)

58% aller Datendiebstähle gingen auf Aktivistengruppen zurück

Es überrascht nicht wirklich, dass Außenstehende nach wie vor für den Datenklau in Unternehmen hauptverantwortlich sind. Organisierte Kriminelle führten ihre typischen Verbrechen im Schilde und steckten hinter der Mehrzahl der Verstöße im Jahr 2011. Aktivistengruppen hatten ebenfalls im vergangenen Jahr ihren „gerechten“ Anteil an Unbill und Wirrnis – und sie stahlen mehr Daten als jede andere Gruppe. Ihr Auftritt diente auch dazu, die Landschaft in gewisser Weise zu verändern, was die Absichten hinter den Datenverletzungen angeht. Während die guten alten Bekannten Gier und Geiz nach wie vor die Hauptgründe waren, nahmen ideologischer Protest und Schadenfreude eine prominentere Rolle unter den registrierten Fällen ein. Wie bei solch einer Zunahme an Angreifern von außen zu erwarten, verringerte sich der prozentuale Anteil von Verstößen durch Insider weiter bis zu vergleichsweise geringen 4 %.

WIE ENTSTEHEN DATENVERLETZUNGEN?

Verstöße im Zusammenhang mit Hacking und Malware nahmen im vergangenen Jahr beträchtlich zu, wobei Hacking mit nahezu allen kompromittierten Datensätzen in Verbindung stand. Dies ergibt insofern einen Sinn, als Außenstehende, die hinter den meisten dieser Vorfälle stehen, diese Tools nach wie vor bevorzugen. Viele Angriffe vereiteln oder umgehen weiterhin die Authentisierung, indem sie gestohlene oder erratene persönliche Daten (um Zugang zu erhalten) mit Backdoors (um den Zugang zu behalten) kombinieren. Weniger Betrugsfälle an Geldautomaten oder Tankstellen in diesem Jahr führten dieser Studie zufolge zu einer Senkung der Rate physischer Angriffe. Angesichts der geringeren Zahl interner Angreifer fiel die Kategorie Missbrauch zwangsläufig ebenfalls niedriger aus. Social-Engineering-Taktiken kamen etwas seltener vor, sind jedoch für eine große Menge an Datenverlusten verantwortlich.

81% nutzten Hacking in irgendeiner Form (+31 %)

69% verwendeten Malware (+20 %)

10% gingen mit physischen Angriffen einher (-19 %)

7% setzten Social-Engineering-Taktiken ein (-4 %)

5% resultierten aus dem Missbrauch von Zugriffsberechtigungen (-12 %)

WELCHE GEMEINSAMKEITEN BESTEHEN?

79% der Opfer waren Gelegenheitsziele (-4 %)

96% der Angriffe waren nicht sehr komplex (+4 %)

94% aller Datenverletzungen kamen von Servern (+18 %)

85% der Verstöße wurden erst nach Wochen oder später entdeckt (+6 %)

92% der Vorfälle wurden von einer Drittpartei entdeckt (+6 %)

97% der Verstöße wären durch einfache oder intermediäre Kontrollen vermeidbar gewesen (+1 %)

96% der Betroffenen hatten keine PCI-DSS-Compliance erreicht (+7 %)

Die Ergebnisse aus dem vergangenen Jahr zeigen erneut, dass die Wahl des Angriffsziels eher eine Frage der Gelegenheit ist, als der gezielten Auswahl. Die meisten fielen den Angreifern zum Opfer, weil sie eine (häufig leicht) ausnutzbare Schwäche besaßen, und nicht, weil sie vorher als potenzielles Opfer identifiziert worden waren.

Egal ob gezielt oder nicht, die große Mehrheit der Opfer erlag Angriffen, die nicht als sonderlich komplex bezeichnet werden können. Diejenigen, die eher eine Tendenz zur Komplexität aufwiesen, offenbarten diese Eigenschaft in der Regel erst zu einem späteren Zeitpunkt des Angriffs, nachdem der Erstzugang bereits erfolgt war.

Daher nimmt es nicht wunder, dass die meisten Sicherheitsverletzungen vermeidbar gewesen wären (zumindest im Nachhinein) und zwar ohne aufwändige oder teure Gegenmaßnahmen. Eine mangelhafte PCI-DSS-Compliance deutet auf eine Vielzahl an Problemen aller Art bei den betroffenen Unternehmen hin.

Wenngleich häufig zumindest einige Hinweise auf Sicherheitsverletzungen vorhanden sind, entdecken Opfer ihre eigenen Vorfälle zumeist nicht. Gewöhnlich machen Dritte sie darauf aufmerksam, und leider geschieht dies typischerweise erst Wochen oder Monate später.

Ist Ihnen aufgefallen, dass sich die Situation im Jahr 2011 in den meisten Fällen verschlechtert hat?

WORAUF SOLLTEN SICH PRÄVENTIONSMASSNAHMEN KONZENTRIEREN?

Wie gesagt, diese Studie erinnert uns daran, dass unser Berufsstand über die notwendigen Werkzeuge verfügt, um Datenverletzungen erfolgreich anzugehen. Die Herausforderung an die Guten liegt in der Wahl der richtigen Werkzeuge für die anstehende Aufgabe und darin, sie dann nicht achtlos liegen zu lassen, bis sie Rost ansetzen. Es gibt hinreichend Nachweise dafür, dass die Bösen sehr schnell Nutzen daraus ziehen.

Wie Sie bald sehen werden, stellen wir die Ergebnisse kleinerer und größerer Unternehmen im Laufe dieses Berichts einander gegenüber. Sie werden eine Vorstellung davon bekommen, wie unterschiedlich (und in einigen Fällen wie ähnlich) deren Probleme zumeist sind. Deswegen ist es sinnvoll, dass die Lösungen für diese Probleme ebenfalls unterschiedlich sind. So beziehen sich die meisten Empfehlungen, die wir am Schluss dieses Berichts geben, auf größere Unternehmen. Es ist nicht so, dass wir die Kleinen außer Acht lassen – es ist bloß so, dass es, obwohl die moderne Cyberkriminalität ihnen schwer zu schaffen macht, ein recht einfaches und nahezu universell einsetzbares Gegenmittel gibt.

Größere Unternehmen weisen ein breiteres Spektrum an Problemen auf, die man mit einer ebenso vielfältigen Palette an Lösungsmaßnahmen angehen muss. Eine auf Ihre Bedürfnisse zugeschnittene Lösungsstrategie erfordert jedoch eine wissensbasierte und gründliche Untersuchung Ihrer individuellen Bedrohungssituation.

Kleinere Unternehmen

- ✓ Implementieren Sie eine Firewall oder Zugriffssteuerungsliste für Remote-Zugangsdienste.
- ✓ Ändern Sie die voreingestellten Zugangsdaten von POS-Systemen und anderen mit dem Internet verbundenen Geräten.
- ✓ Wenn ein externer Dienstleister die oben genannten Punkte übernimmt, stellen Sie sicher, dass sie wirklich umgesetzt wurden.

Größere Unternehmen

- ✓ Löschen Sie überflüssige Daten; behalten Sie die verbleibenden im Auge
- ✓ Stellen Sie sicher, dass wesentliche Kontrollen durchgeführt werden, und überprüfen Sie dies regelmäßig.
- ✓ Überwachen und analysieren Sie Ereignisprotokolle.
- ✓ Bewerten Sie Ihre Bedrohungssituation, um die Prioritäten für Ihre Lösungsstrategie festzulegen.
- ✓ Konsultieren Sie die Schlussfolgerungen aus diesem Bericht, um Anzeichen und Präventionsmaßnahmen für die häufigsten Bedrohungen zu finden.

THREAT-EVENT-ÜBERSICHT

Im Vorjahres-DBIR stellten wir das mit Häufigkeitszählungen ausgefüllte *Threat-Event*-Raster von VERIS zum ersten Mal vor. Neben den neuen Partnern, die ihre Daten mit uns teilten, gehörte dies zu den Aspekten des Berichts, die am meisten Anklang fanden. Die Statistiken in diesem Bericht bieten eine separate Analyse der beobachteten *Agents*, *Actions*, *Assets* und *Attributes*, aber das hier gezeigte Raster verknüpft alles miteinander und zeigt dadurch die Schnittpunkte zwischen den „vier A“. Es vermittelt eine Gesamtübersicht der spezifischen Bedrohungsereignisse, die mit den Datenverletzungen aus 2011 in Zusammenhang stehen. Abbildung 1 (gesamter Datensatz) und Abbildung 2 (größere Unternehmen) verwenden die Struktur von Abbildung 1 aus dem Abschnitt über die Methode im Gesamtbericht, ersetzen jedoch die TE-Nummern mit der Gesamtanzahl der Datenverletzungen, in denen jedes spezifische Bedrohungsereignis Teil des Störfallszenarios war³. Dies ist unsere am stärksten konsolidierte Ansicht der in diesem Jahr analysierten 855 Datenverletzungen, und es sind einige Dinge beachtenswert.

Betrachtet man den kompletten Datensatz aus dem Blickwinkel des Bedrohungsmanagements, so zeigt sich, dass nur 40 der 315 *Threat Events* einen Wert haben, der größer als 0 ist (13 %). Bevor wir fortfahren, möchten wir noch einmal darauf hinweisen, dass nicht alle Schnittpunkte auf dem Raster realisierbar sind. Es sei nochmals erwähnt, dass dieser Bericht sich allein auf Datenverletzungen konzentriert. Im Rahmen der Projekte, bei denen wir mit Unternehmen zusammengearbeitet haben, um ihre kompletten Sicherheitsvorfälle im Laufe eines Jahres zu „VERIS-ieren“, war es interessant zu beobachten, wie unterschiedlich diese Raster im Vergleich zu den DBIR-Datensätzen aussehen. Wie man vermuten mag, kommen die Kategorien Fehler und Missbrauch sowie Verfügbarkeitsverluste weitaus häufiger vor.

Die Ergebnisse in Bezug auf den Gesamtdatensatz weisen viele Ähnlichkeiten mit unserem letzten Bericht auf. Die größten Veränderungen bestehen darin, dass Missbrauch und physische Angriffe etwas an Bedeutung verloren haben, während Malware und Hacking gegen Server und Endanwendergeräte eindeutig die Oberhand gewonnen haben.

Doch zurück zu den Rastern, deren Ergebnisse in Bezug auf die Gesamtdatensätze viele Ähnlichkeiten mit unserem letzten Bericht aufweisen. Die größten Veränderungen bestehen darin, dass Missbrauch und physische Angriffe etwas an Bedeutung verloren haben, während Malware und Hacking gegen Server und Endanwendergeräte eindeutig die Oberhand gewonnen haben. Genauso scheint die Liste der häufigsten Bedrohungen in Tabelle 3 unheimlich vertraut.

³ Mit anderen Worten: 381 der 855 Datenverletzungen im Jahr 2011 standen in Zusammenhang mit externer Malware, die die Vertraulichkeit eines Servers beeinträchtigte (das *Threat Event* ganz oben links).

Abbildung 1. VERIS-A⁴-Raster, das die Häufigkeit der *Threat Events* der obersten Ebene abbildet

		Malware			Hacking			Sozial			Missbrauch			Physisch			Fehler			Umweltbedingt		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Server	Vertraulichkeit & Eigentum	381			518		1				9	8	1				2	1				
	Integrität & Authentizität	397			422		1				6	1	1									
	Verfügbarkeit & Nutzen	2			6						5											
Netzwerke	Vertraulichkeit & Eigentum										1											
	Integrität & Authentizität	1									1											
	Verfügbarkeit & Nutzen	1			1						1											
Endgeräte	Vertraulichkeit & Eigentum	356			419						1			86								
	Integrität & Authentizität	355			355						1	1		86								
	Verfügbarkeit & Nutzen										1			3								
Offline-Daten	Vertraulichkeit & Eigentum											23						1				
	Integrität & Authentizität																					
	Verfügbarkeit & Nutzen																					
Menschen	Vertraulichkeit & Eigentum							30	1													
	Integrität & Authentizität							59	2													
	Verfügbarkeit & Nutzen																					

Wenn man die in Abbildung 2 separat dargestellten Bedrohungen in größeren Unternehmen betrachtet, ergeben sich einige weitere Diskussionspunkte. Manche mögen überrascht sein, dass diese Version des Rasters weniger „gefüllt“ ist als in Abbildung 1 (22 der 315 Ereignisse – 7% – wurden mindestens einmal beobachtet). Man würde erwarten, dass die größere Angriffsfläche und strengere Kontrollen in größeren Unternehmen die Angriffe auf einen größeren Teil des Raster ausbreiten lassen würden. Das mag zutreffen, und unsere Ergebnisse sollten nicht dazu dienen, um diesen Aspekt zu widerlegen. Wir meinen, dass die geringere Dichte in Abbildung 2 im Vergleich zu Abbildung 1 in erster Linie eine Folge der Größenunterschiede in den Datensätzen ist (855 gegenüber 60 Datenverletzungen). Mit Blick auf die Bedrohungsvielfalt ist es interessant zu beobachten, dass das Raster für größere Unternehmen eine vergleichsweise gleichmäßigere Verteilung der spezifischen Bedrohungen aufweist (d. h. eine weniger extreme Zusammenballung bei Malware und Hacking). Angesichts der Beschreibungen von spektakulären Angriffen in der Presse, bei denen Formen des Social Engineering zum Einsatz kamen, ist das nicht schockierend.

Selbstverständlich werden die Bedrohungsfaktoren, -handlungen und Assets, die in den Datenverletzungen des Jahres 2011 eine Rolle spielten, im vollständigen Bericht wesentlich detaillierter erforscht. Er liefert auch zusätzliche Informationen zur Datenerfassungsmethode von Verizon und den anderen Mitwirkenden.

Abbildung 2. VERIS-A⁴-Raster, das die Häufigkeit der *Threat Events* der obersten Ebene abbildet - GRÖßERE UNTERNEHMEN

		Malware			Hacking			Sozial			Missbrauch			Physisch			Fehler			Umweltbedingt		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Server	Vertraulichkeit & Eigentum	7			33						3						2	1				
	Integrität & Authentizität	10			18						1											
	Verfügbarkeit & Nutzen				1																	
Netzwerke	Vertraulichkeit & Eigentum																					
	Integrität & Authentizität																					
	Verfügbarkeit & Nutzen	1			1																	
Endgeräte	Vertraulichkeit & Eigentum	3			6									10								
	Integrität & Authentizität	4			2									10								
	Verfügbarkeit & Nutzen													1								
Offline-Daten	Vertraulichkeit & Eigentum										1							1				
	Integrität & Authentizität																					
	Verfügbarkeit & Nutzen																					
Menschen	Vertraulichkeit & Eigentum							7														
	Integrität & Authentizität							11														
	Verfügbarkeit & Nutzen																					

2012 DBIR: SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

In diesem Jahr haben wir etwas Neues in diesen Abschnitt aufgenommen. Da wir jedoch so ein umweltbewusster Konzern sind, recyceln wir zunächst noch einmal die folgenden Informationen:

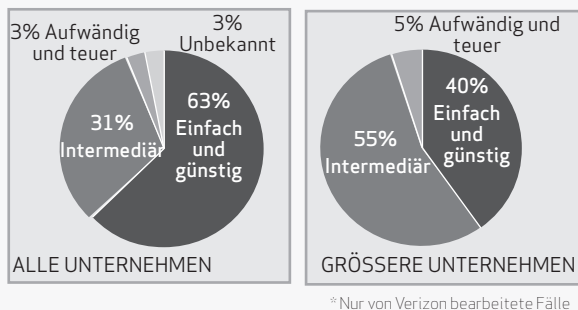
„Die Erstellung einer Liste von zuverlässigen Empfehlungen gestaltet sich mit jedem Jahr, in dem wir diesen Bericht veröffentlichen, schwieriger. Denken Sie darüber nach: Unsere Ergebnisse verändern und entwickeln sich mit der Zeit, doch selten sind sie völlig neu oder unerwartet. Warum sollten daher die Empfehlungen, die auf diesen Ergebnissen basieren, abweichen? Natürlich könnten wir improvisieren und eine lange Liste von Maßnahmen entwerfen, um eine Quote zu erfüllen, doch wir glauben, dass Sie das auch woanders bekommen können. Wir sind mehr an Qualität als an Quantität interessiert.“

Anschließend kürzen und verwenden wir einen Teil des Materials aus dem 2009 Supplemental DBIR noch einmal und schreiben ihn so um, dass er hoffentlich hilfreich für Sie ist. Wie erwähnt haben wir auch etwas Neues produziert, aber dabei darauf geachtet, unsere CO₂- (und Papier-) Bilanz nicht über Gebühr zu strapazieren. Wenn Sie dies mit der Energie kombinieren, die durch die Vermeidung von Reisen der Ermittler, dem Versand von Beweisen und unzähligen Datenverarbeitungszyklen eingespart wird, dann haben sich diese Empfehlungen wirklich ihre grüne Plakette verdient.

Fangen wir mit dem „etwas Neuen“ an. Wir sind zu der Erkenntnis gelangt, dass viele der Unternehmen, die Gegenstand dieses Berichts sind, die Botschaft über ihre Sicherheit wahrscheinlich nicht erhalten. Wir sprechen von den kleineren Unternehmen, die ein oder nur eine Handvoll POS-Systeme betreiben. Der folgende Ausschnitt

wurde speziell für sie entworfen, und wir brauchen dafür Ihre Hilfe. Wir laden Sie, unsere Leser, dazu ein, ihn herauszutrennen und an Restaurants, Einzelhändler, Hotels oder andere Einrichtungen, die Sie frequentieren, weiterzugeben. Dadurch helfen Sie uns, die Botschaft zu verbreiten, die diese Unternehmen hören sollten. Ganz zu schweigen davon, dass es sich um eine Botschaft handelt, die der Rest von uns auch hören sollte. Diese Tipps mögen simpel erscheinen, aber alle uns zur Verfügung stehenden Belege deuten darauf hin, dass ein großer Teil des Problems in kleineren Unternehmen gelöst wäre, wenn sie gängige Praxis werden würden.

Abbildung 3. Kosten der empfohlenen präventiven Maßnahmen anhand des Prozentsatzes an Datenverletzungen*



Der folgende Ausschnitt wurde speziell für kleinere Unternehmen entworfen, und wir brauchen dafür Ihre Hilfe. Wir laden Sie, unsere Leser, dazu ein, ihn herauszutrennen und an Restaurants, Einzelhändler, Hotels oder andere Einrichtungen, die Sie frequentieren, weiterzugeben.



POINT-OF-SALE-SICHERHEITSTIPPS

Guten Tag. Sie haben diese Karte erhalten, weil jemand Ihre Einrichtung schätzt. Jemand, der Ihnen dabei helfen möchte, Ihr Unternehmen ebenso zu schützen wie seine Zahlungsdaten und persönlichen Informationen.

Es mag einfach sein zu denken: „Das wird mir nie passieren!“, wenn es um die Frage geht, ob Hacker Ihre Daten stehlen könnten. Vielleicht wird es Sie überraschen zu hören, dass sich die meisten Angriffe gegen kleine Unternehmen richten und die meisten mit ein paar kurzen und einfachen Schritten verhindert werden können. Unten finden Sie ein paar Tipps, die auf den Nachforschungen von Verizon in tausenden von Sicherheitsverletzungen beruhen, in denen Unternehmen betroffen waren, die Point-of-Sale (POS)-Systeme für die Zahlungsabwicklung verwenden. Wenn Sie mit dieser Information nichts anfangen können, geben Sie diesen Ausschnitt bitte an Ihre Geschäftsleitung weiter.

- ✓ **Ändern Sie administrative Passwörter auf allen POS-Systemen.**
 - Hacker scannen das Internet nach leicht zu erratenden Passwörtern.
- ✓ **Implementieren Sie eine Firewall oder Zugriffssteuerungsliste für Remote-Access/Administrations-Services.**
 - Wenn Hacker Ihr System nicht erreichen, können sie von dort nicht einfach etwas stehlen.

Anschließend könnten folgende Maßnahmen für Sie in Betracht kommen:

- Vermeiden Sie es, POS-Systeme für das Browsen im Internet zu verwenden (das gilt übrigens auch für alle andere Aktivitäten im Internet).
- Stellen Sie sicher, dass Ihr POS-System eine PCI-DSS-konforme Anwendung ist (fragen Sie Ihren Anbieter danach).

Wenn ein externer Anbieter Ihre POS-Systeme betreut, bitten Sie ihn um Bestätigung, dass die genannten Maßnahmen umgesetzt wurden. Wenn möglich, lassen Sie sich die entsprechende Dokumentation aushändigen. Wenn Sie diese einfachen Praktiken befolgen, ersparen Sie Ihrem Unternehmen und Ihren Kunden jede Menge Geld, Zeit und Ärger.

Weitere Informationen finden Sie unter www.verizonbusiness.com/de/Products/security/dbir (aber bitte nicht von Ihrem POS aus).

Für all diejenigen, die sich nicht mehr daran erinnern: Der 2009 Supplemental DBIR war eine Art Lexikon der häufigsten damals beobachteten Gefahren. Jeder Eintrag enthielt eine Beschreibung, damit verbundene Bedrohungsfaktoren, betroffene Assets, Indikatoren, Maßnahmen zur Schadensminderung sowie eine Fallstudie. Um größeren Unternehmen relevante und umsetzbare Empfehlungen an die Hand zu geben, verwenden wir aus jenem Bericht den Teil über die „Indikatoren“ und „Maßnahmen zur Schadensminderung“ hier zu einem anderen Zweck.

- **Indikatoren:** Warnsignale und Kontrollmechanismen, die entdecken oder anzeigen, dass sich eine Bedrohungshandlung anbahnt oder vorgefallen ist.
- **Maßnahmen zur Schadensminderung:** Kontrollmechanismen, die Bedrohungshandlungen abwehren oder verhindern oder im Nachgang zur Wiederherstellung/Reaktion (Eindämmung des Schadens) beitragen können.

Unsere Empfehlungen leiten wir aus Tabelle 7 ab, die sich in dem Abschnitt mit der Übersicht über die Bedrohungshandlungen findet und die zehn wichtigsten Bedrohungshandlungen gegenüber größeren Unternehmen zeigt. Anstelle die ganze Liste hier noch einmal zu wiederholen, fassen wir die Punkte, die in unseren Augen die größten Gelegenheiten bieten, unser gemeinsames Risiko eines Datenverlusts zu senken, zusammen:

- Keylogger und die Verwendung gestohlener persönlicher Zugangsdaten
- Backdoors und Befehlskontrolle
- Manipulation
- Pretexting
- Phishing
- Brute-Force-Methode
- SQL-Injection

Hacking: Verwendung gestohlener Zugangsdaten	
Beschreibung	Bezieht sich auf Situationen, in denen ein Angreifer Zugang zu einem geschützten System oder Gerät erlangt, indem er gültige, aber gestohlene Zugangsdaten verwendet.
Indikatoren	Vorhandensein von Malware im System; Analyse des Nutzerverhaltens weist auf Anomalien hin (d. h. Ursprungsort oder Anmeldezeit sind anormal); Verwendung des „Last Logon“-Banners (weist möglicherweise auf unbefugten Zugriff hin); Überwachung sämtlicher administrativer/privilegierter Aktivitäten.
Maßnahmen zur Schadensminderung	Doppelte Authentifizierung; Passwortänderung bei Verdacht auf Diebstahl; Regeln für die Nutzungszeit; IP-Blacklisting (erwägen, ob man große Adressblöcke/Regionen blockiert, wenn sie keinem legitimen Geschäftszweck dienen); Verbindungen für administrative Aufgaben einschränken (d. h. nur von bestimmten internen Ressourcen aus zulassen). Wie man den Diebstahl von Zugangsdaten verhindert, lesen Sie in den Einträgen unter <i>Keylogger und Spyware</i> , <i>Pretexting</i> und <i>Phishing</i> .
Malware: Backdoors, Command-and-Control-Technologien	
Hacking: Ausnutzen des Backdoor- oder Command-and-Control-Kanals	
Beschreibung	Tools, die Remote-Zugriff zu und/oder von infizierten Systemen bieten. Backdoors und Command-and-Control-Programme umgehen normale Authentifizierungsmechanismen und andere Sicherheitskontrollen, die in einem System eingerichtet wurden und so konzipiert sind, dass sie im Verborgenen ablaufen.

Malware: Backdoors, Command-and-Control-Technologien

Hacking: Ausnutzen des Backdoor- oder Command-and-Control-Kanals

Indikatoren	Anomalien bei Verhalten oder Performance des Systems (mehrere Opfer beobachteten, wie sich der Cursor zwischen Dateien hin und her bewegte, ohne dass jemand die Maus berührte); ungewöhnliche Netzwerkaktivität; IDS/IPS (bei nicht spezifisch angepassten Versionen); Registrierungsüberwachung; Überwachung der Systemprozesse; Routineüberwachung von Logdaten; Vorhandensein anderer Malware im System; AV deaktiviert. Im Laufe der Ermittlungen in Bezug auf vermutete Malware untersuchen wir gemeinhin die aktiven Systemprozesse und erstellen eine Liste aller Systeminhalte, die nach dem Datum der Erstellung/Modifikation sortiert ist. Diese Bemühungen fördern häufig bössartige Dateien in den Windows\system32- und den temporären Verzeichnissen zutage.
Maßnahmen zur Schadensminderung	Egress-Filtering (diese Tools werden oft über ungerade Ports, Protokolle und Services betrieben); Verwendung von Proxys für ausgehenden Verkehr; IP-Blacklisting (erwägen, ob man große Adressblöcke/Regionen blockiert, wenn sie keinem legitimen Geschäftszweck dienen); Host-IDS (HIDS) oder Integritätsüberwachung; die administrativen Rechte der Nutzer einschränken; Data-Loss-Prevention-Tools (DLP); Antiviren- und Anti-Spyware-Programme (obgleich die stärkere individuelle Anpassung AV weniger wirksam werden lässt – wir haben eine Backdoor entdeckt, die nur von einem aus 40 AV-Anbietern, die wir getestet haben, erkannt wurde); Richtlinien für das Browsen im Web.

Physisch: Manipulation

Beschreibung	Unberechtigte Änderung oder Störung des normalen Zustands oder Betriebs eines Assets. Bezieht sich auf physische Formen der Manipulation im Gegensatz zur Änderung der Software oder der Systemeinstellungen.
Indikatoren	Eine ungeplante oder außerplanmäßige Wartung des Geräts. Vorhandensein von Kratzern, Klebstoffresten, Löchern für Kameras oder einer Tastaturaufklage. Erwarten Sie nicht, dass die Manipulation offensichtlich ist (Skimming-Vorsätze können maßgefertigt sein und sich so nahtlos in ein bestehendes Gerät einfügen, während interne Manipulationen von außen unsichtbar geschehen können). Das Sicherheitssiegel kann beschädigt sein. In manchen Fällen kann ein unbekanntes Bluetooth-Signal vorhanden sein und bestehen bleiben. Bedenken Sie, dass Skimming-Geräte an Geldautomaten/Zapfsäulen möglicherweise nur einige Stunden angebracht bleiben und nicht Tage oder Wochen.
Maßnahmen zur Schadensminderung	Schulen Sie Mitarbeiter und Kunden darin Zeichen von Manipulation zu suchen und aufzuspüren. Unternehmen, die solche Geräte betreiben, sollten diese mehrmals am Tag untersuchen (z. B. beim Schichtwechsel). Bei der Inspektion sollten Sie daran denken, dass bei einem Gerät, das die Eingabe von Karte und PIN verlangt, generell beide gefährdet sind (siehe Indikatoren). Legen sie für alle Mitarbeiter eine Vorgehensweise für den Umgang mit Servicetechnikern fest, und schulen Sie sie entsprechend; stellen Sie sicher, dass dies eine Methode für die zeitliche Planung und die Authentifizierung von Technikern oder Wartungsfirmen umfasst. Bestehen Sie bei Ihren Anbietern auf Anti-Manipulationstechnologien/-Funktionen, oder erwerben Sie nur POS- und PIN-Geräte mit dieser Technologie (z. B. Schutzkontakte, die den Speicher löschen, mit Epoxid versiegelte Elektronik).

Keylogger/Form-Grabber/Spyware

Beschreibung	Malware, die speziell dafür bestimmt ist, die Handlungen eines Systemnutzers zu erfassen, zu überwachen und zu protokollieren. Wird typischerweise dazu verwendet, um Nutzernamen und Passwörter als Teil eines größeren Angriffsszenarios zu sammeln. Dient auch dazu, um Kreditkarteninformationen auf kompromittierten POS-Geräten zu erfassen. Die meisten laufen im Verborgenen ab, um den Nutzer nicht zu warnen, dass seine Handlungen überwacht werden.
Indikatoren	Anomalien bei Verhalten oder Performance des Systems; ungewöhnliche Netzwerkaktivität, IDS/IPS (bei nicht spezifisch angepassten Versionen); Registrierungsüberwachung; Überwachung der Systemprozesse; Routineüberwachung von Logdaten; Vorhandensein anderer Malware im System; Zeichen von physischer Manipulation (z. B. Anbringen eines fremden Geräts). Für Anzeichen, dass abgeschöpfte Zugangsdaten verwendet wurden, siehe <i>Hacking: Verwendung gestohlener Zugangsdaten</i> . Im Laufe der Ermittlungen in Bezug auf vermutete Malware untersuchen wir gemeinhin die aktiven Systemprozesse und erstellen eine Liste aller Systeminhalte, die nach dem Datum der Erstellung/Modifikation sortiert sind. Diese Bemühungen fördern häufig bössartige Dateien in den Windows\system32- und den temporären Verzeichnissen zutage.
Maßnahmen zur Schadensminderung	Schränken Sie Administrationsrechte der Nutzer ein; Code Signing; Verwendung von Live-Boot-CDs, Einmalpasswörtern, Antiviren- und Anti-Spyware-Programmen, Personal Firewalls; Filtern von Webinhalt und Blacklisting; Egress-Filtering (diese Tools versenden oft Daten anhand ungerader Ports, Protokolle und Services); Host-IDS (HIDS) Integritätsüberwachung; Richtlinien für das Browsen im Web; Schulung des Sicherheitsbewusstseins; Netzwerksegmentierung.

Pretexting (Social Engineering)

Beschreibung	Eine Social-Engineering-Technik, bei der ein Angreifer ein Szenario erfindet, um den Betroffenen zu überreden, zu manipulieren oder zu täuschen, damit dieser eine Handlung ausführt oder Informationen preisgibt. Diese Angriffe nutzen „Fehler in der menschlichen Hardware“ aus, und leider gibt es dafür keinen Patch.
Indikatoren	Sehr schwer aufzuspüren, da der Zweck darin besteht, menschliche Schwächen auszunutzen, und technologische Alarmmechanismen umgangen werden. Ungewöhnliche Mitteilungen, Anfragen außerhalb des normalen Workflows und die Aufforderung Informationen herauszugeben oder Maßnahmen entgegen den Richtlinien zu ergreifen, sollten als verdächtig eingestuft werden. Anrufprotokolle; Besucherprotokolle; E-Mail-Protokolle.
Maßnahmen zur Schadensminderung	Allgemeine Schulung zur Steigerung des Sicherheitsbewusstseins; klar definierte Richtlinien und Abläufe; „trainieren“ Sie Ihre Mitarbeiter nicht darauf, Richtlinien zu missachten, indem Sie selbst diese Richtlinien durch offizielle Handlungen übertreten; schulen Sie Mitarbeiter darin, mutmaßliche Versuche eine falsche Identität vorzutäuschen, zu erkennen und zu melden; überprüfen Sie verdächtige Anfragen anhand vertrauenswürdiger Methoden und Kanäle; begrenzen Sie den öffentlichen Zugriff auf Unternehmensverzeichnisse (und ähnliche Informationsquellen).

Brute-Force-Angriff

Beschreibung	Ein automatisierter Prozess, bei dem so lange alle möglichen Nutzernamen-Passwort-Kombinationen durchprobiert werden, bis eine erfolgreich ist.
---------------------	---

Brute-Force-Angriff	
Indikatoren	Routineüberwachung von Logs; zahlreiche misslungene Login-Versuche (besonders diejenigen, die auf ein mehrfach wiederholtes Erraten hindeuten); Anrufe beim Helpdesk wegen gesperrter Accounts.
Maßnahmen zur Schadensminderung	Technische Mittel zur Erzwungung von Passwortrichtlinien (Länge, Komplexität, Clipping-Levels); Kontensperrung (nach x Versuchen); Passwort-Throttling (längere Verzögerungszeit nach aufeinanderfolgenden Fehlversuchen); Passwort-Knacker-Tests; Zugriffssteuerungslisten; Verbindungen für administrative Aufgaben einschränken (d. h. nur von bestimmten internen Ressourcen aus zulassen); Zwei-Wege-Authentifizierung; CAPTCHA.
SQL-Injection	
Beschreibung	SQL-Injection ist eine Angriffstechnik, die verwendet wird, um die Art, wie Webseiten mit Backend-Datenbanken kommunizieren, auszunutzen. Ein Angreifer kann einer Datenbank Befehle (in Form von speziell angefertigten SQL-Statements) erteilen, indem er die Eingabefelder auf einer Website nutzt.
Indikatoren	Routineüberwachung von Logs (insbesondere Webserver und Datenbank); IDS/IPS.
Maßnahmen zur Schadensminderung	Sichere Entwicklungsprinzipien; Input-Validierung (Einsatz von Maskierungszeichen und Whitelists); Verwendung parametrisierter und/oder gespeicherter Abläufe; Least-Privilege-Prinzipien für Datenbank-Accounts anwenden; Entfernung von überflüssigen Dienstleistungen; System-Hardening; Ausgabe von Datenbank-Fehlermeldungen an den Client deaktivieren; Schwachstellentests von Webanwendungen; Penetrationstests; Firewall für Webanwendungen.
Unberechtigter Zugang mittels Standardzugangsdaten	
Beschreibung	Bezieht sich auf Vorfälle, bei denen ein Angreifer Zugang zu einem System oder Gerät erhält, das durch standardmäßig voreingestellte (und daher weithin bekannte) Nutzernamen und Passwörter geschützt ist.
Indikatoren	Analyse des Nutzerverhaltens (z. B. anomaler Ursprungsort oder Anmeldezeit); Überwachung sämtlicher administrativer/privilegierter Aktivitäten; Verwendung des „Last Logon“-Banners (weist möglicherweise auf unbefugten Zugriff hin).
Maßnahmen zur Schadensminderung	Standardeinstellungen der Zugangsdaten ändern (vor dem Deployment); Standard-Account löschen oder deaktivieren; nach bekannten Standardpasswörtern suchen (nach dem Deployment); Passwort-Rotation (weil es hilft, den Wechsel der Standardeinstellung zu forcieren); Inventarisierung der Remote-Verwaltungsdienste (besondere diejenigen, welche durch dritte Parteien geleistet werden). Für Dritte: Verträge (Vereinbarung von Passwort-Richtlinien); eventuell administrative Aufgaben teilen; Suche nach bekannten Standardpasswörtern (bei Assets, die von Dritten betreut werden).
Phishing (und zahllose andere *ishing-Variationen)	
Beschreibung	Eine Social-Engineering-Technik, bei der der Angreifer betrügerische, elektronische Kommunikation (in der Regel E-Mail) dazu einsetzt, um den Empfänger dazu zu verleiten, Informationen preiszugeben. Die meisten erwecken den Eindruck, dass sie von einem rechtmäßigen Unternehmen stammen und enthalten authentisch wirkenden Inhalt. Der Angriff umfasst oft neben dem Köder eine gefälschte Website-Komponente.

Phishing (und zahllose andere *ishing-Variationen)

Indikatoren	Schwer zu entdecken wegen des quasi-technischen Charakters und der Fähigkeit, menschliche Schwächen auszunutzen. Unerbetene und ungewöhnliche Mitteilungen; Aufforderung Informationen herauszugeben oder Maßnahmen entgegen den Richtlinien zu ergreifen; Anfragen außerhalb des normalen Workflows; Grammatikfehler; das Erzeugen eines Gefühls der Dringlichkeit; E-Mail-Logs.
Maßnahmen zur Schadensminderung	Allgemeine Schulung zur Steigerung des Sicherheitsbewusstseins; klar definierte Richtlinien und Abläufe; „trainieren“ Sie Ihre Mitarbeiter nicht darauf, Richtlinien zu missachten, indem Sie diese Richtlinien selbst durch offizielle Handlungen übertreten; Richtlinien für die Verwendung von E-Mails für administrative Aufgaben (z. B. Passwortänderungsanfragen usw.); schulen Sie Mitarbeiter darin, mutmaßliche Phishing-Nachrichten zu erkennen und zu melden; überprüfen Sie verdächtige Anfragen anhand vertrauenswürdiger Methoden und Kanäle; konfigurieren Sie E-Mail-Clients so, dass sie HTML-E-Mails als Text übermitteln; Anti-Spam; Virenüberprüfung und Filtern von E-Mail-Anhängen.



2012 DATA BREACH INVESTIGATIONS REPORT

Eine vom Verizon RISK-Team durchgeführte Studie in Zusammenarbeit mit der australischen Bundespolizei, der niederländischen High Tech Crime Unit, dem irischen Reporting & Information Security Service, der Police Central e-Crime Unit der London Metropolitan Police und dem United States Secret Service



verizon.com/enterprise/de

© 2012 Verizon. Alle Rechte vorbehalten. MC15244 DE 05/12. Die Namen und Logos Verizon und Verizon Business sowie sonstige Namen, Logos und Slogans, die auf Produkte und Dienstleistungen von Verizon verweisen, sind Marken oder Dienstleistungsmarken der Verizon Trademark Services LLC oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern. Sämtliche anderen erwähnten Marken und Dienstleistungsmarken sind Eigentum der jeweiligen Rechteinhaber.