WPROWADZENIE

Komputery są integralną częścią naszej infrastruktury gospodarczej, społecznej, zawodowej, rządowej i militarnej. Stały się one niezbędne w praktycznie każdej dziedzinie współczesnego życia, ale ich podatność na włamania jest coraz bardziej niepokojąca. Systemy komputerowe są stale zagrożone nieumyślnym błędem i działaniami natury, a także tymi, które można przypisać nieetycznym, niemoralnym i kryminalnym działaniom. Celem naszym jest dostarczenie wskazówek dotyczących rozpoznawania tych zagrożeń, eliminacja ich tam, gdzie to możliwe, a jeśli nie, redukowanie przypisywanych im strat. Blog będzie najbardziej wartościowy dla osób bezpośrednio odpowiedzialnych za bezpieczeństwo komputerów, sieci lub informacji, a także tych, którzy muszą zaprojektować, zainstalować i utrzymywać bezpieczne systemy. Będzie to równie ważne dla tych menedżerów, na których funkcje operacyjne mogą mieć wpływ naruszenia bezpieczeństwa, oraz dla tych kierowników, którzy są odpowiedzialni za ochronę powierzonych im aktywów. Wraz z pojawieniem się komputerów stacjonarnych, przenośnych i netbooków oraz z rozległymi sieciami międzynarodowymi, które je łączą, natura i zasięg zagrożeń dla bezpieczeństwa komputerowego wzrosły niemalże poza miarę.

BEZPIECZEŃSTWO SYSTEMU INFORMACYJNEGO

Rozwój komputerów i technologii informatycznych był wybuchowy. Nigdy wcześniej technologia na całym świecie nie była propagowana z taką szybkością i z tak wielką penetracją praktycznie każdej ludzkiej działalności. Komputery przyniosły ogromne korzyści w tak różnorodnych dziedzinach, jak badania genomu człowieka, eksploracja kosmosu, sztuczna inteligencja i wiele aplikacji od trywialnych do najbardziej poprawiających jakość życia. Niestety, komputery mają też ciemną stronę: są używane do projektowania i budowania broni masowego rażenia, a także samolotów wojskowych, atomowych łodzi podwodnych i rozpoznawczych stacji kosmicznych. Rola komputera w formułowaniu broni biologicznej i chemicznej oraz w symulacji ich rozmieszczenia jest jednym z najmniej pomyślnych zastosowań. Z nieco mniejszym niepokojem komputery wykorzystywane w aplikacjach finansowych, takie jak ułatwianie kupowania i sprzedaży wszystkiego, od zapałek do rezydencji i przekazywanie bilionów dolarów każdego dnia w elektronicznych funduszach, są nieodparte dla złoczyńców; wielu z nich postrzega te działania jako otwarte zaproszenia do oszustw i kradzieży. Systemy komputerowe i ich wzajemnie połączone sieci są również ofiarami wandali, złośliwych egotyków, terrorystów oraz szeregu osób, grup, firm i rządów zamierzających wykorzystać je do realizacji własnych celów, całkowicie ignorując wpływ na niewinne ofiary. . Poza celowymi atakami na systemy komputerowe istnieją niezliczone sposoby, w których niezamierzone błędy mogą uszkodzić lub zniszczyć zdolność komputera do wykonywania zamierzonych funkcji. Wzrost bezpieczeństwa systemów informatycznych był podobny do samego pola komputerowego. Tylko dzięki szczegółowej analizie potencjalnych problemów i implementacji proponowanych rozwiązań można oczekiwać, że komputery spełnią swoją obietnicę, przy niewielu lukach bezpieczeństwa, które nękają mniej odpowiednio zabezpieczone systemy.

Bezpieczeństwo można zdefiniować jako stan wolny od niebezpieczeństwa i nie narażony na uszkodzenia spowodowane wypadkami lub atakiem, lub można go określić jako proces osiągania tego pożądanego stanu. Celem systemu bezpieczeństwa informacji jest optymalizacja działania organizacji w odniesieniu do zagrożeń, na które jest ona narażona. Ryzyko definiuje się jako ryzyko obrażeń, uszkodzenia lub utraty. Ryzyko składa się zatem z dwóch elementów: (1) przypadku - elementu niepewności oraz (2) potencjalnej straty lub uszkodzenia. Z wyjątkiem możliwości restytucji, podjęte dziś działania w zakresie bezpieczeństwa systemów informatycznych działają w celu zmniejszenia przyszłych strat ryzyka. Ze względu na niepewność co do przyszłych strat ryzyka, doskonałe bezpieczeństwo, które oznacza zerowe straty, byłoby nieskończenie kosztowne. Z tego powodu osoby

zarządzające ryzykiem dążą do optymalizacji alokacji zasobów, minimalizując całkowity koszt podjętych środków bezpieczeństwa systemu informacyjnego i poniesionych strat. Ten proces optymalizacji jest zwykle nazywany zarządzaniem ryzykiem. Zarządzanie ryzykiem w tym sensie jest trzyczęściowym procesem:

1. Identyfikacja istotnych zagrożeń
2. Wybór i wdrażanie środków ograniczających ryzyko
3. Śledzenie i ocena poniesionych strat ryzyka w celu zatwierdzenia dwóch pierwszych części procesu

ZARZĄDZANIE RYZYKIEM

Było częścią biznesu od stuleci. Kupcy renesansowi często używali kilku statków jednocześnie, z których każdy przewoził część towaru, tak że utrata jednego statku nie spowodowałaby utraty całej partii. Niemal w tym samym czasie rozwinęła się koncepcja ubezpieczeń, po pierwsze, aby zapewnić ekonomiczną ochronę przed utratą ładunku, a następnie zapewnić ochronę przed utratą budynków przez pożar. Ubezpieczyciele od ognia i władze miejskie zaczęli wymagać przestrzegania norm mających na celu zmniejszenie ryzyka katastrof takich jak Wielki Pożar Londynu w 1666 roku. W 1667 roku powstał w Londynie Instytut Ubezpieczeń. Wraz z pojawieniem się korporacji jako spółek akcyjnych z ograniczoną odpowiedzialnością, dyrektorzy korporacyjni byli zobowiązani do stosowania ostrożności i należytej staranności w ochronie aktywów akcjonariuszy. Zagrożenia związane z bezpieczeństwem należą do zagrożonych aktywów korporacyjnych, które dyrektorzy mają obowiązek rozwiązać.

PODWÓJNE KSIĘGOWANIE

Kolejny renesansowy wynalazek, okazał się doskonałym narzędziem do mierzenia i kontrolowania aktywów korporacyjnych. Jednym z celów było utrudnienie ukrywania oszustw poufnych. Pojawiła się koncepcja rozdziału obowiązków, w której wezwano do stosowania procedur przetwarzania, które wymagały więcej niż jednej osoby do zrealizowania transakcji. Ponieważ księgi rachunkowe nabierają coraz większego znaczenia, opracowano standardy rachunkowości i nadal ewoluują one do dnia dzisiejszego. Standardy te służyły do porównywania ksiąg rachunkowych i zapewnienia osobom postronnym, że księgi rachunkowe organizacji prezentują dokładny obraz stanu i aktywów. Te zmiany doprowadziły z kolei do wymogu niezależnego przeglądu ksiąg rachunkowych i procedur operacyjnych przez zewnętrznego audytora. Przejście na automatyczne systemy księgowe wprowadziło dodatkowe wymagania bezpieczeństwa. Niektóre wczesne zabezpieczenia, takie jak zasada przeciwko wymaganiom lub zmianom w księgach rachunkowych, już nie są stosowane. Niektórym skomputeryzowanym systemom księgowym brakowało śladu rewizyjnego, a inne mogły być tak samo przekierowane, jak rzeczywiste wpisy. Wreszcie, wraz z nadejściem Ery Informacji, własność intelektualna stała się coraz ważniejszą częścią korporacyjnych i rządowych aktywów. W tym samym czasie, gdy własność intelektualna zyskała na znaczeniu, zagrożenia dla własności intelektualnej stały się bardziej niebezpieczne ze względu na samą technologię systemu informacyjnego (IS). Kiedy poufne informacje były przechowywane na papierze i innych dokumentach materialnych, a szybkie kopiowanie było ograniczone do fotografii, ochrona była stosunkowo prosta. Niemniej jednak, systemy kontroli dokumentów, procedury klasyfikacji informacji i niezbędne kontrole dostępu nie były niezawodne, a pojawiały się kompromisy w informacjach z konsternacją regularności. Ewolucja technologii IS sprawiła, że kontrola informacji była o kilka rzędów wielkości bardziej złożona. Ewolucja i, co ważniejsze, wdrażanie technik kontroli nie dotrzymują kroku. Opiszemy, w jaki sposób ewolucja systemów informatycznych spowodowała równoległą ewolucję bezpieczeństwa systemu informatycznego, a jednocześnie zwiększyła znaczenie przewidywania wpływu nadchodzących zmian

technicznych. Przegląd ten wyjaśni czynniki prowadzące do dzisiejszego środowiska zagrożeń bezpieczeństwa systemu informatycznego i technik ograniczania ryzyka i posłuży jako ostrzeżenie, aby pozostać czujnym na implikacje innowacji technicznych w momencie ich pojawiania się.

EWOLUCJA SYSTEMÓW INFORMATYCZNYCH

Pierwszy elektromechaniczny system kart perforowanych do przetwarzania danych, opracowany przez Hermana Holleritha pod koniec XIX wieku, został wykorzystany do zestawienia w tabelach i całkowitych raportach ze spisu powszechnego w Amerykańskim Biurze Spisu Powszechnego w 1890 roku. Pierwsze cyfrowe komputery z zainstalowanym programem opracowane w 1940 roku zostały wykorzystane do celów wojskowych, głównie kryptoanalizy oraz obliczania i drukowania tabel do strzelania przez artylerię. W tym samym czasie systemy kart perforowanych były już wykorzystywane do zastosowań księgowych i były oczywistym wyborem dla danych na wejście na nowe elektroniczne maszyny obliczeniowe

Lata 50-te : Systemy kart perforowanych

W latach 50. sprzęt komputerowy z kartami perforowanymi dominował na rynku komputerów komercyjnych. Te elektromechaniczne urządzenia mogą wykonywać pełen zakres funkcji księgowych i raportujących. Ponieważ zostały zaprogramowane przez skomplikowany system wtyczek z wieloma kablami wtyczkowymi, a także dlatego, że podczas obsługi i przechowywania kart perforowanych trzeba było zachować ostrożność, w pobliżu urządzenia mogły przebywać tylko doświadczone osoby. Chociaż którakolwiek z tych osób mogła założyć sprzęt do nieuczciwego użycia, a nawet zaangażować się w sabotaż, najwyraźniej niewielu, jeśli w ogóle, faktycznie to zrobiło. Systemy księgowania z kartami dziurkowanymi zwykle stosowały cztery etapy przetwarzania. Na wstępie operatorzy otrzymają "paczkę" dokumentów, zazwyczaj z dodaną taśmą maszynową pokazującą jedną lub więcej "sum kontrolnych". Operator wpisał dane każdego dokumentu do karty dziurkowanej, a następnie dodał dodatkową kartę, kontrolną kartę wsadową, przechowującą sumy partii. Każda karta składała się z 80 kolumn, z których każda zawiera najwyżej jeden znak. Kompletny zapis elementu z inwentaryzacji, na przykład, byłby zawarty na pojedynczej karcie. Kartę nazwano kartą jednostkową, a maszyny nazywane były albo jednostkowymi rekordami, albo automatami do kart perforowanych. Było to spowodowane koniecznością wciśnięcia jak największej ilości danych na 80-znakową kartę, z której powstał późniejszy problem roku 2000. Kompresowanie roku na dwie postacie było uniwersalnym użytym środkiem oszczędzający miejsce; jej konsekwencje 40 lat później nie były przewidziane. Grupa kart perforowanych, zwana również "partią", była zwykle trzymana na metalowej tacy. Czasami partia byłaby powtórnie dziurkowana przez drugiego operatora, korzystającego raczej z "trybu weryfikacji", niż z wykrawania nowych dziur w kartach, w celu wykrycia błędów klawisza przed przetwarzaniem talii kart. Każda partia kart byłaby przetwarzana osobno, więc procesy były określane jako "zadania wsadowe". Pierwszym krokiem byłoby uruchomienie partii kart za pomocą prostego programu, który obliczyłby sumy kontrolne i porównał je z sumami na karcie kontrolnej partii. Jeśli sumy partii nie zostały uzgodnione, partia została odesłana z powrotem do obszaru klawiszy w celu ponownego uruchomienia. Jeśli sumy się zgodzą, talia zostanie scalona z innymi partiami tego samego typu transakcji, na przykład obecna lista płac. Po zakończeniu tego kroku nowa partia składała się z karty perforowanej dla każdego pracownika w kolejności zatrudnienia. Program płacowy zaakceptował tę talię kart danych wejściowych i przetwarzał karty jeden po drugim. Każda karta została dopasowana do odpowiedniej karty pracownika w talii menedżerów płac, aby obliczyć bieżące wynagrodzenie netto i wyszczególnione odliczenia oraz przebić nową kartę główną płac, w tym sumy z roku na rok. Ostatnim krokiem było wykorzystanie talii kart do drukowania czeków płacowych i raportów zarządczych. Kroki te były identyczne z tymi stosowanymi przez wczesne, małe komputery elektroniczne. Jedyną różnicą była szybkość, z jaką dokonano rzeczywistych obliczeń. Kompletny proces był nadal znany jako zadanie

wsadowe. Dzięki temu procesowi potencjał do nadużyć był wielki. Operator maszyny może kontrolować każdy etap operacji. Chociaż dane były wbijane do kart i weryfikowane przez innych, w pobliżu znajdował się automat do keypingu do wykorzystania przez operatora maszyny. Teoretycznie ta osoba może przebić nową kartę płac i nową kartę zbiorczą, aby dopasować zmianę przed wydrukowaniem czeków. Niska częstość zgłoszonych exploitów wynikała z kontroli, które zniechęcały do takich nadużyć i prawdopodobnie z dumy, jaką operatorzy maszyn doświadczyli w swoich zawodach.

KOMUTERY WIELKOSKALOWE

Podczas gdy te elektromechaniczne maszyny z dziurkowanymi kartami były sprzedawane w dużych ilościach, laboratoria badawcze i uniwersytety pracowały nad zaprojektowaniem wielkoskalowych komputerów, które miałyby rewolucyjny wpływ na całą dziedzinę. Te komputery, zbudowane na lampach próżniowych, znane są jako pierwsza generacja. W marcu 1951 r. Amerykański Uniwersalny Komputer Automatyczny (UNIVAC) został zaakceptowany przez amerykańskie Biuro ds. Spisu Ludności (Census Bureau). Do tej pory każdy komputer był projektem jednorazowym, ale UNIVAC był pierwszym masowo produkowanym komputerem, w sumie zbudowano ich 46. Słowo "uniwersalny" w nazwie wskazuje, że UNIVAC był również pierwszym komputerem zaprojektowanym do zastosowań naukowych i biznesowych. UNIVAC zawierał 5200 lamp próżniowych, ważył 29 000 funtów i zużywał 125 kilowatów energii elektrycznej. Dozowano z perforowanymi kartami, odbierając dane wejściowe z metalowej taśmy o szerokości 0,5 cm, nagranej z klawiatury, z wyjściem na podobną taśmę lub do drukarki. Chociaż nie jest to model dla przyszłych projektów, jego pamięć składała się z 1000 72-bitowych słów i została wykonana jako rtęciowa linia opóźniająca. Mieścił się w szafie o wysokości około sześciu stóp, szerokości dwóch stóp i głębokości dwóch stóp, wypełnionej rtęcią cewki biegnącej od góry do dołu. Przetwornik na górze propagował wolno poruszające się fale energii wzdłuż cewki do przetwornika odbierającego na dole. Tam został ponownie przetworzony na energię elektryczną i przekazany do odpowiedniego obwodu lub recyrkulowany, jeśli wymagane było dłuższe przechowywanie. W 1956 r. IBM wprowadził magnetyczny system dyskowy Random Access Method of Accounting and Control (RAMAC). Składał się z 50 magnetycznie powlekanych metalowych tarcz o średnicy 24 cali, zamontowanych na wspólnym wrzecionie. Pod serwosterowaniem dwie połączone głowice do odczytu / zapisu przesuwają się po każdej stronie wymaganego dysku, a następnie do wewnątrz, do dowolnej ze 100 ścieżek. W jednym obrocie dysków można odczytać lub nagrać wszystkie lub prawie wszystkie informacje na tych dwóch ścieżkach. Cały system był prawie wielkości kompaktowego samochodu i utrzymywał to, co w tym czasie stanowiło ogromną ilość danych - 5 megabajtów. Koszt wyniósł 10 000 USD za megabajt lub 35 000 USD rocznie za dzierżawę. W porównaniu z niektórymi dzisiejszymi magnetycznymi dyskami twardymi, które mierzą około 31/2 cali szerokości i wysokości 1 cala, przechowują nawet 1000 gigabajtów i kosztują mniej niż 400 USD lub około 0,0004 USD na megabajt. Te wczesne, masywne komputery były umieszczone w dużych , klimatyzowanych pokojach. W pomieszczeniu kilku doświadczonych ekspertów, wyglądających na bardzo profesjonalnych w białych fartuchach laboratoryjnych, brało udział w operacjach i utrzymaniu opłat za milion dolarów. Nie istniała koncepcja "użytkownika" jako osoby spoza komputera, która mogłaby wchodzić w interakcje bezpośrednio z maszyną. Przerwy w usługach, błędy oprogramowania i błędy sprzętowe zazwyczaj nie są krytyczne. Jeśli którykolwiek z nich spowodował awarię lub przerwanie programu, rozpoczęcie od nowa było stosunkowo proste. W związku z tym podstawowymi problemami związanymi z bezpieczeństwem były: fizyczna ochrona rzadkiego i kosztownego sprzętu oraz środki zwiększające ich niezawodność. Kolejną kwestią, tak jak teraz, była ludzka omylność. Ponieważ najwcześniejsze komputery były programowane w niezwykle trudnym języku maszynowym, składającym się wyłącznie z jedynek (1) i zer (0), częstość występowania błędów ludzkich była wysoka, a czas korekty błędów był zbyt długi. Dopiero później opracowano języki asemblera i kompilatora w

celu zwiększenia liczby osób zdolnych do programowania maszyn i zmniejszenia częstości występowania błędów oraz czasu na ich poprawienie. Bezpieczeństwo systemu informatycznego dla dużych komputerów nie stanowiło istotnego problemu z dwóch powodów. Po pierwsze, niewielu programistów potrafiło wykorzystywać i manipulować komputerami. Po drugie, było bardzo mało komputerów, z których każdy był niezwykle cenny, ważny dla właścicieli, a co za tym idzie ściśle strzeżony

KOMPUTER ŚREDNIEJ WIELKOŚCI

W latach pięćdziesiątych opracowano mniejsze systemy komputerowe o bardzo prostej konfiguracji; Pliki wzorcowe kart perforowanych zostały zastąpione perforowaną taśmą papierową, a następnie taśmą magnetyczną i systemami przechowywania dysków. Kalkulator elektromechaniczny wraz z jego płytką został zastąpiony przez centralny procesor (CPU), który miał małą pamięć główną, czasami zaledwie 8 kilobajtów, 4 i ograniczoną szybkość przetwarzania i moc. Jeden lub dwa czytniki kart perforowanych mogą odczytywać dane i instrukcje przechowywane na tym nośniku. Później programy i pliki danych były przechowywane na taśmie magnetycznej. Dane wyjściowe zostały przesłane do kart maszyn, do drukowania na urządzeniu rejestrującym urządzenia, a później do taśmy magnetycznej. Wciąż nie ma połączenia przewodowego ze światem zewnętrznym i nie ma użytkowników online, ponieważ nikt, oprócz osób zajmujących się przetwarzaniem danych elektronicznych (EDP) w pokoju komputerowym, nie może bezpośrednio wchodzić w interakcje z systemem. Te systemy miały bardzo proste systemy operacyjne i nie używały wieloprocesowości; mogły uruchamiać tylko jeden program na raz. Model IBM 650, wprowadzony w 1954 roku, mierzył około 5 stóp na 3 stopy na 6 stóp i ważył prawie 2000 funtów. Jego zasilacz został zamontowany w podobnej wielkości szafce, ważącej prawie 3000 funtów. Zawierał 2000 (10-cyfrowy) słów pamięci głównej bębna magnetycznego o łącznej wartości 500 000 USD lub czynszu w wysokości 3 200 USD miesięcznie. Za dodatkowe 1500 USD miesięcznie można by dodać znacznie szybszą pamięć rdzenia o 60 słowach. Dane wejściowe i wyjściowe wykorzystywały maszyny do odczytu i zapisu kart dziurkowanych. Typowy sprzęt IS z lat 50. XX wieku został zainstalowany w oddzielnym pomieszczeniu, często z oknem podglądowym, aby goście mogli podziwiać komputer. We wczesnej próbie bezpieczeństwa, odwiedzający faktycznie w sali komputerowej byli często witani wydrukowanym napisem:

Achtung! Alles Lookenspeepers!

Das computermachine ist nicht fur gefingerpoken und mittengrabben.

Ist easy schnappen der springenwerk, blowenfusen, und poppencorken mit spitzensparken.

Ist nicht fur gewerken bei das dumbkopfen.

Das rubbernecken sightseeren keepen hans in das pockets muss. Relaxen und watch das blinkenlichten.

Ponieważ nadal nie było użytkowników online, nie było żadnych identyfikatorów użytkowników ani haseł. Programy przetwarzają partie danych, uruchamiane w regularnych odstępach czasu - raz dziennie, raz w tygodniu itd., W zależności od funkcji. Jeśli dane dla programu nie były dostępne w zaplanowanym czasie uruchomienia, operatorzy mogliby zamiast tego uruchomić inne zadanie i czekać na brakujące dane. Ponieważ raporty wydruków stały się dostępne, zostały dostarczone ręcznie do użytkowników końcowych. Użytkownicy końcowi nie spodziewali się ciągłego przepływu danych z systemu przetwarzania informacji, a opóźnienia nawet o dzień lub więcej nie były znaczące, z wyjątkiem być może z produkcją wypłaty. Bezpieczeństwo systemu informatycznego prawie nie było

uważane za takie. Nacisk położono na kontrole wsadowe dla poszczególnych programów, fizyczne kontrole dostępu i utrzymanie odpowiedniego środowiska dla niezawodnej pracy sprzętu

LATA 60-TE : KOMPUTERY O MAŁEJ SKALI

W latach sześćdziesiątych, przed wprowadzeniem komputerów na małą skalę, terminale dumb udostępniały użytkownikom klawiaturę do wysyłania strumienia znaków do komputera i ekran wideo, który może wyświetlać znaki przesyłane do niego przez komputer. Początkowo terminale te były używane, aby pomóc operatorom komputerów kontrolować i monitorować strumień zadań, zastępując banki przełączników i kontrolek na konsoli sterowania. Wkrótce uznano jednak, że terminale te mogą zastąpić także czytniki kart i klawiatury. Teraz użytkownicy, identyfikowani przez identyfikatory użytkowników i uwierzytelniani za pomocą haseł, mogli wprowadzać dane wejściowe przez terminal CRT do programu edycji, który sprawdzałby dane wejściowe, a następnie zapisywał je na twardym dysku, dopóki nie był potrzebny do przetwarzania. Później zdano sobie sprawę, że użytkownicy mają także bezpośredni dostęp do danych przechowywanych w internetowych plikach głównych.

TRANYSTORY I PAMIĘĆ RDZENIA

IBM 1401, wprowadzony w 1960 roku z pamięcią rdzeniową o wielkości 4096 znaków, był pierwszym całkowicie tranzystorowym komputerem, oznaczającym nadejście drugiej generacji. Mieści się w szafce o wymiarach 5 stóp na 3 stopy . 1401 wymagało podobnej szafy, aby dodać dodatkowe 12 kilobajtów pamięci głównej. Zaledwie rok później pierwsze układy scalone zostały wykorzystane w komputerze, co było możliwe wszystkie przyszłe postępy w miniaturyzowaniu małych komputerów i znaczne zmniejszenie wielkości komputerów mainframe

PODZIAŁ CZASU

W 1961 roku opracowano system Compatible Time Sharing (CTSS) dla IBM 7090/7094. To oprogramowanie systemu operacyjnego i związany z nim sprzęt były pierwszymi, które zapewniają równoczesny zdalny dostęp do grupy użytkowników online poprzez multiprogramowanie. "Multiprogramming" oznacza, że więcej niż jeden program może pojawić się w tym samym czasie. Główny program sterujący, zwykle nazywany systemem operacyjnym (OS), zarządzał wykonywaniem aplikacji funkcjonalnych. Na przykład, pod komendą operatora, system operacyjny załaduje się i uruchomi aplikację nr 1. Po 50 milisekundach system operacyjny przerywałby wykonywanie aplikacji nr 1 i zapisywał jej bieżący stan w pamięci. Wtedy system operacyjny uruchomi aplikację nr 2 i pozwoli na uruchomienie przez 50 milisekund, i tak dalej. Zwykle, w ciągu sekundy po tym, jak użytkownicy wprowadzili dane z klawiatury, system operacyjny dałby swoim aplikacjom wycinek czasu do przetworzenia danych wejściowych. Przy każdym wycinku czasowym komputer może wykonać setki instrukcji. Te techniki sprawiły, że komputer był w całości poświęcony programowi każdego użytkownika. Było to prawdą tylko o tyle, o ile liczba jednoczesnych użytkowników była dość mała. Potem, gdy liczba wzrosła, reakcja na każdego użytkownika zwolniła.

SYSTEM CZASU RZECZYWISTEGO

Ze względu na multi programowanie i możliwość przechowywania rekordów online i dostępnych w losowej kolejności stało się możliwe zapewnienie użytkownikom końcowym bezpośredniego dostępu do danych. Na przykład system rezerwacji linii lotniczych przechowuje zapis każdego miejsca na każdym locie przez następne 12 miesięcy. Urzędnik dokonujący rezerwacji, pracujący w terminalu, może odpowiedzieć na telefoniczne zapytanie, wyszukać dostępne miejsce na konkretny lot, podać cenę biletu, sprzedać bilet dzwoniącemu i zarezerwować miejsce. Podobnie funkcjonariusz banku

może zweryfikować saldo rachunku i dokonywać przelewów pieniężnych. W obu przypadkach dostęp do każdego rekordu danych może być natychmiastowy i zmieniony, a nie konieczności oczekiwania na uruchomienie partii. Do dnia dzisiejszego zarówno urzędnik rezerwujący, jak i funkcjonariusz banku mogą zostać zastąpieni przez samych klientów, którzy bezpośrednio kontaktują się z komputerami online. Chociaż postęp ten doprowadził do znacznego zwiększenia dostępnej mocy obliczeniowej, znacznie zwiększył również ryzyko naruszenia zabezpieczeń komputera. W przypadku bardziej złożonych systemów operacyjnych, gdy wielu użytkowników korzysta z Internetu w newralgicznych programach, a także z baz danych i innych plików dostępnych dla nich, należy zapewnić ochronę przed przypadkowym błędem i zamierzonym nadużyciem.

RODZINA KOMPUTERÓW

W 1964 roku IBM ogłosił rodzinę komputerów S / 360, od bardzo małych do bardzo dużych modeli. Wszystkie z sześciu modeli wykorzystywały układy scalone, które oznaczały początek trzeciej generacji komputerów. Tam, gdzie tranzystorowa konstrukcja może pozwolić na 6000 tranzystorów na stopę sześcienną, 30 000 układów scalonych może zajmować taką samą objętość. To znacznie obniżyło koszty, a firmy mogły kupić rodzinę po cenie w granicach swoich możliwości. Ponieważ wszystkie komputery z tej serii używały tego samego języka programowania i tych samych urządzeń peryferyjnych, firmy mogły w razie potrzeby aktualizować je z łatwością. Rodzina 360 szybko zdominowała rynki handlowe i naukowe. W miarę jak komputery te mnożyły się, podobnie jak liczba użytkowników, doświadczonych programistów i techników. Z biegiem lat opracowano techniki i procesy, aby zapewnić wysoki poziom bezpieczeństwa dla tych systemów mainframe. W roku 1964 pojawił się także inny komputer o dalekosiężnych wpływach: Digital Equipment Corp. (DEC) PDP-8. PDP-8 był pierwszym masowo produkowanym prawdziwym minikomputerem. Chociaż pierwotna aplikacja była w trakcie kontroli procesu, PDP-8 i jego potomstwo szybko udowodniły, że komercyjne aplikacje dla minikomputerów były praktycznie nieograniczone. Ponieważ komputery te nie były izolowane w bezpiecznych pomieszczeniach komputerowych, ale były rozprowadzane w wielu niestrzeżonych biurach w szeroko rozproszonych lokalizacjach, pojawiły się zupełnie nowe zagrożenia, wymagające innowacyjnych rozwiązań.

CUDOWNE LATA SIEDEMDZIESIĄTE

Lata 70. XX wieku: Mikroprocesory. Podstawy wszystkich obecnych komputerów osobistych (PC) zostały ustanowione w 1971 roku, kiedy Intel wprowadził komputer 4004 na chipie. Mierząc 1/16 cala i 1/8 cala wysokości, 4004 zawierał 2250 tranzystorów z zegarem 108 kHz. Obecna generacja tego najwcześniejszego programowalnego mikroprocesora zawiera miliony tranzystorów, z prędkościami powyżej 1 gigaHertz lub ponad 10 000 razy szybciej. Wprowadzenie chipów mikroprocesorowych oznaczało czwartą generację.

Pierwsze komputery osobiste: Prawdopodobnie pierwszy komputer osobisty był reklamowany w Scientific American w 1971 roku. KENBAK-1, wyceniony na 750 $, miał trzy rejestry programujące, pięć trybów adresowania i 256 bajtów pamięci. Chociaż niewiele ich sprzedano, KENBACK-1 zwiększył świadomość publiczną na temat możliwości domowych komputerów. To MITS Altair 8800 stał się pierwszym komputerem osobistym do sprzedaży w znacznych ilościach. Podobnie jak KENBACK-1, Altair 8800 miał tylko 256 bajtów pamięci, ale był wyceniony na 375 USD bez klawiatury, wyświetlacza lub dodatkowej pamięci. Około roku później Apple II, zaprojektowane przez Steve'a Jobsa i Steve'a Wozniaka, miało cenę 1 998 USD, w tym wyświetlacz CRT i klawiaturę. Ponieważ te pierwsze komputery osobiste były całkowicie autonomiczne i zwykle znajdowały się pod kontrolą pojedynczej osoby, było kilka problemów związanych z bezpieczeństwem. Jednak w 1978 roku opracowano program arkusza kalkulacyjnego VisiCalc. Zalety standaryzowanych, niedrogich, szeroko stosowanych

programów aplikacyjnych były niekwestionowane, ale pakiety programów, w przeciwieństwie do niestandardowych projektów, otworzyły drogę do nadużyć, ponieważ tak wiele osób rozumiało ich interfejsy użytkownika, a także ich wewnętrzne działania.

Pierwsza sieć : Sieć krajowa, stworzona pod koniec 1969 roku, narodziła się jako ARPANET (Advanced Research Projects Agency Network), sponsorowana przez Departament Obrony, mająca na celu połączenie kilku ważnych uniwersytetów badawczych w kraju. Miała dwa cele: rozwijanie doświadczenia w łączeniu komputerów i zwiększanie produktywności dzięki współużytkowaniu zasobów. To najwcześniejsze połączenie niezależnej wielkiej skali systemy komputerowe miały zaledwie cztery węzły: University of California w Los Angeles (UCLA), University of California w Santa Barbara, Stanford Research Institute i University of Utah. Ze względu na nieodłączne bezpieczeństwo każdego węzła połączonego z linią dzierżawioną oraz fizycznie chronione pomieszczenia komputerowe typu mainframe, nie było wyraźnej troski o kwestie bezpieczeństwa. To była ta prosta sieć, bez myśli o bezpieczeństwie, z której wyewoluował dzisiejszy wszechobecny Internet i Internet (WWW), z ich ogromnym potencjałem na nadużycia w zakresie bezpieczeństwa.

Dalsze kwestie dotyczące bezpieczeństwa : Wraz z rozprzestrzenianiem się zdalnych terminali na komputerach komercyjnych, fizyczna kontrola dostępu do sali komputerowej przestała być wystarczająca. W odpowiedzi na nowe luki opracowano logiczne systemy kontroli dostępu. System kontroli dostępu utrzymuje tablicę online autoryzowanych użytkowników. Typowy rekord użytkownika zapisywałby nazwę użytkownika, numer telefonu, numer pracownika oraz informacje o danych, do których użytkownik był uprawniony, oraz o programach, do których wykonania użytkownik był uprawniony. Użytkownik może mieć możliwość przeglądania, dodawania, modyfikowania i usuwania rekordów danych w różnych kombinacjach dla różnych programów. W tym samym czasie menedżerowie systemu uznali wartość możliwości odzyskania po awarii, która zniszczyła sprzęt i dane. Centra danych zaczęły tworzyć regularne kopie taśmowe plików online i oprogramowania do przechowywania poza siedzibą. Kierownicy centrów danych zaczęli także opracowywać i wdrażać plany usuwania skutków awarii z zewnątrz, często z wykorzystaniem komercyjnych urządzeń do odtwarzania po awarii. Nawet przy takim systemie, nowe luki zostały rozpoznane w kolejnych latach i są one przedmiotem wielu podręczników.

Pierwszy "robak" : Prorocza powieść science-fiction, The Shockwave Rider, autorstwa Johna Brunnera (1975), przedstawiła "robaka", który nieustannie rósł w sieci komputerowej. Robak ostatecznie przekroczył miliard bitów długości i stał się niemożliwe do zabicia bez zniszczenia sieci. Chociaż rzeczywiste robaki (np. Morris Worm z 1988 r.) stały się później rzeczywistymi zagrożeniami dla wszystkich komputerów w sieci, rozważny personel bezpieczeństwa komputerowego instaluje stale aktualizowane programy antymalware, które skutecznie zabijają wirusy i robaki bez konieczności zabijania sieci.

80 LAT MINĘŁO JAK JEDEN DZIEŃ …

1980: Poprawa wydajności : Dekada lat osiemdziesiątych może być nazwana erą poprawy produktywności. Instalacja milionów komputerów osobistych w komercyjnych, przemysłowych i rządowych aplikacjach zwiększyła wydajność i funkcjonalność ogromnej liczby użytkowników. Zaliczki te, które można było osiągnąć w żaden inny sposób, nie zostały wykonane na kosztach, na które praktycznie każdy mógł sobie pozwolić.

1980: Komputer osobisty : W 1981 r. IBM wprowadził niewielki komputer o ogólnym przeznaczeniu, zwany "komputerem osobistym". Ten model i podobne systemy stały się ogólnie znane jako komputery osobiste. Do tej pory małe komputery były produkowane przez stosunkowo nieznane źródła, ale IBM, z ogólnoświatową reputacją, wprowadził komputery osobiste do głównego nurtu. Fakt, że IBM wykazał

wiarę w rentowność komputerów osobistych, uczynił z nich poważnych pretendentów do użytku korporacyjnego. Było wiele wariacje na temat podstawowego modelu 5100 PC, a sprzedaż wzrosła daleko poza szacunkami IBM. Podstawowa konfiguracja wykorzystywała Intel 8088, pracujący z szybkością 4,77 megaherca, z maksymalnie dwoma stacjami dyskietek, każdy o pojemności 160 kilobajtów iz dyskowym systemem operacyjnym (DOS) w otwartej architekturze. Ta otwarta architektura systemu operacyjnego, z dostępnymi "hakami", umożliwiła rozwój niezależnych producentów oprogramowania, z których najważniejszym był Microsoft Corporation, utworzony przez Billa Gatesa i Paula Allena. IBM zlecił Gatesowi i Allenowi stworzenie systemu operacyjnego DOS. Zgodnie z umową IBM nie zwróci Gatesowi i Allenowi kosztów związanych z opracowaniem; raczej wszystkie zyski ze sprzedaży DOS zostaną im naliczone. IBM nie miał wyłącznego prawa do systemu operacyjnego, a Microsoft zaczął go sprzedawać wielu innym klientom jako MS-DOS. Początkowo IBM dołączał do swojego komputera program arkusza kalkulacyjnego VisiCalc, ale wkrótce sprzedaż Lotus 1-2-3 przekroczyła możliwości VisiCalc. Otwarta architektura nie tylko umożliwiła wielu programistom tworzenie oprogramowania, które działałoby na komputerze, ale także umożliwiłoby każdemu zestawienie zakupionych komponentów w komputerze, który byłby konkurencyjny w stosunku do komputera IBM. Szybki rozwój zgodnych programów aplikacyjnych w połączeniu z gotową dostępnością zgodnego sprzętu wkrótce doprowadził do sprzedaży ponad 1 miliona sztuk. Wiele kolejnych generacji oryginalnego sprzętu i oprogramowania nadal generuje sprzedaż mierzoną w milionach rocznie. Apple podchodzi do bardzo odmiennego podejścia do swojego komputera Macintosh. Tam, gdzie system IBM był szeroko otwarty, Apple utrzymywał ścisłą kontrolę nad dowolnym sprzętem lub oprogramowaniem zaprojektowanym do działania na Macintoshu, aby zapewnić kompatybilność i łatwość instalacji. Najważniejszymi innowacjami Apple były graficzny interfejs użytkownika (GUI) i mysz, które współpracowały ze sobą, aby ułatwić łatwość użycia, a obie zostały uzyskane z badań i rozwoju w Stanford Research Institute i Xerox Palo Alto Research Institute w lata sześćdziesiąte i siedemdziesiąte. Microsoft w 1985 r. Podjął próbę zbudowania tych funkcji w systemie operacyjnym Windows, ale wcześniejsze wersje były na ogół odrzucane jako powolne, uciążliwe i niewiarygodne. Dopiero w 1990 roku Windows 3.0 pokonał wiele problemów i zapewnił podstawę dla późniejszych wersji, które były niemal powszechnie akceptowane.

Sieci lokalne : W latach 80. samodzielne komputery stacjonarne zaczęły przetwarzać tekst, analizę finansową i przetwarzanie grafiki. Chociaż takie rozwiązanie było znacznie wygodniejsze dla użytkowników końcowych niż scentralizowany obiekt, trudniej było dzielić się danymi z innymi. W miarę rozwoju potężniejszych komputerów, praktyczne stało się ich łączenie, aby ich użytkownicy mogli łatwo udostępniać dane. Ustalenia te były powszechnie nazywane sieciami lokalnymi (LAN), ponieważ jednostki sprzętowe były fizycznie blisko, zwykle w tym samym budynku lub w obszarze biurowym. LAN pozostały ważne do dziś. Zwykle jako serwer plików wyznaczono bardziej wydajny komputer z dyskiem o dużej pojemności. Inne komputery, nazywane stacjami roboczymi, zostały podłączone do serwera plików za pomocą kart interfejsu sieciowego zainstalowanych na stacjach roboczych za pomocą kabli między tymi kartami a serwerem plików. Specjalne oprogramowanie sieciowe zainstalowane na serwerze plików i stacjach roboczych umożliwiło stacjom roboczym dostęp do określonych części dysku twardego serwera plików tak, jakby te części były zainstalowane na stacjach roboczych. Co więcej, te współużytkowane pliki można zarchiwizować na serwerze plików bez uzależnienia od indywidualnych użytkowników. W 1997 roku oszacowano, że na całym świecie było ponad 150 milionów komputerów PC pracujących jako stacje robocze LAN. Najpopularniejszymi sieciowymi systemami operacyjnymi (NOS) były Novell NetWare, a później Microsoft IE (Internet Explorer). Większość sieci LAN została zaimplementowana przy użyciu protokołu Ethernet (IEEE 802.3). 10 Serwer i stacje robocze mogą być wyposażone w modem (modulator / demodulator) podłączony do dedykowanej linii telefonicznej. Modem umożliwił użytkownikom zdalnym dostęp do modemu, aby

połączyć się z siecią LAN i zalogować. Była to wielka wygoda dla użytkowników sieci LAN, którzy podróżowali lub pracowali poza biurem, ale taki dostęp zdalny spowodował kolejny nowy problem z bezpieczeństwem. Po raz pierwszy systemy komputerowe zostały w dużym stopniu wystawione na świat zewnętrzny. Odtąd możliwe było współdziałanie z komputerem praktycznie z dowolnego miejsca iz lokalizacji nie znajdujących się pod taką samą kontrolą fizyczną, jak same komputery. Typowe logiczne oprogramowanie kontroli dostępu NOS dla identyfikatorów użytkowników i haseł oraz selektywne uprawnienia dostępu do danych serwera plików i plików programu. Użytkownik stacji roboczej zalogował się do sieci lokalnej, uruchamiając program logowania na serwerze plików. Program poprosił użytkownika o podanie ID i hasła. Jeśli program logowania stwierdził, że identyfikator i hasło są poprawne, sprawdził on w tabeli kontroli dostępu, które dane i programy może uzyskać użytkownik. Zdefiniowano tryby dostępu jako tylko do odczytu, tylko do wykonania, twórz, modyfikuj (zapisuj lub dołączaj), blokuj i usuwaj, w odniesieniu do pojedynczych plików i grup plików. Administrator sieci LAN utrzymywał tablicę kontroli dostępu za pomocą programu narzędziowego. Skuteczność kontroli zależała od staranności administratora, a zatem w niektórych okolicznościach kontrole mogły być słabe. Istotne było zabezpieczenie ID i hasła administratora sieci LAN, ponieważ jeśli zostały naruszone, cały system kontroli dostępu stał się podatny na zagrożenia. Funkcjonariusze ds. Bezpieczeństwa systemów informatycznych zauważyli, że kontrola fizycznego dostępu do serwerów LAN ma kluczowe znaczenie dla utrzymania logicznej kontroli dostępu. Intruzi, którzy mogą fizycznie uzyskać dostęp do serwera sieci LAN, mogą łatwo zrestartować serwer przy użyciu własnej wersji NOS, całkowicie pomijając zainstalowane logiczne kontrole dostępu. Na pozór, sieć LAN wydaje się być taka sama, jak mainframe z lat 70. ze zdalnymi terminalami. Z technicznego punktu widzenia różnica polega na tym, że każdy użytkownik stacji roboczej LAN wykonuje programy na stacji roboczej, a nie na scentralizowanym serwerze plików, podczas gdy komputery mainframe używają specjalnego oprogramowania i sprzętu do jednoczesnego uruchamiania wielu programów, jednego programu dla każdego terminala. Dla użytkownika na stanowisku roboczym lub zdalnym terminalu dwie sytuacje wydają się być takie same, ale z punktu widzenia bezpieczeństwa istnieją znaczne różnice. Oprogramowanie programu mainframe pozostaje na komputerze mainframe i nie może, w normalnych warunkach, zostać zmienione podczas wykonywania. Program LAN na stacji roboczej może zostać zmieniony, na przykład, przez wirusa komputerowego, podczas gdy faktycznie wykonuje. Zasadą jest, że terminale zdalne komputerów mainframe nie mogą pobierać i zapisywać plików, podczas gdy stacje robocze mają zwykle co najmniej napęd dysków wymiennych. Ponadto złośliwy użytkownik stacji roboczej może z łatwością zainstalować urządzenie CD z możliwością wielokrotnego zapisu, co znacznie ułatwia kopiowanie i usuwanie dużych ilości danych. Kolejną ważną różnicą jest charakter połączenia między komputerem a terminalami. Każdy głupi terminal ma dedykowane połączenie z komputerem mainframe i odbiera tylko te dane, które są do niego skierowane. Sieć LAN działa bardziej jak zestaw nadajników radiowych dzielących wspólną częstotliwość, na której serwer plików i stacje robocze na zmianę "przesyłają" wiadomości. Każda wiadomość zawiera blok "nagłówka", który identyfikuje zamierzonego adresata, ale każdy węzeł (serwer plików i stacje robocze) w sieci LAN odbiera wszystkie wiadomości. W normalnych okolicznościach każdy węzeł ignoruje wiadomości, które nie są do niego adresowane. Jest jednak technicznie możliwe, że stacja robocza uruchomi zmodyfikowaną wersję NOS, która pozwoli jej przechwytywać wszystkie wiadomości. W ten sposób stacja robocza może identyfikować wszystkie komunikaty logowania i rejestrować identyfikatory użytkowników oraz hasła wszystkich innych użytkowników w sieci LAN, zapewniając pełny dostęp do wszystkich danych i urządzeń sieci LAN. Bezpieczeństwo systemów mainframe i sieci LAN znacznie różni się także w środowisku operacyjnym. Jak wspomniano, typowy komputer mainframe jest zainstalowany w oddzielnym pomieszczeniu i jest zarządzany przez personel wykwalifikowanych techników. Z drugiej strony, typowy serwer plików LAN jest instalowany w zwykłej przestrzeni biurowej i jest zarządzany przez zdalnie zlokalizowanego administratora sieci LAN, który może nie być odpowiednio przeszkolony.

W związku z tym typowa sieć LAN jest narażona na większe ryzyko manipulacji, sabotażu i kradzieży. Jeśli jednak typowa mainframe zostanie wyłączona w wyniku wypadku, pożaru, sabotażu lub innego incydentu związanego z bezpieczeństwem, wiele funkcji biznesowych zostanie przerwanych, podczas gdy utrata serwera plików sieci LAN zwykle zakłóca tylko jedną funkcję.

KROK DO WSPÓŁCZESNOŚCI

1990: Połączenie międzysystemowe. Usenet rozwinął się na początku lat osiemdziesiątych jako wolny system do publikowania i pobierania wiadomości i komentarzy od uczestników - wczesna forma disintermediacji, ponieważ nie było organów kontrolujących do ograniczania mowy. Grupy dyskusyjne opracowano na każdy możliwy temat, osiągając dziesiątki tysięcy obszarów dyskusji w ciągu kilku lat. Przybyli entuzjaści komputerowi i hakerzy kryminalni do Usenetu jako idealnego kanału do wymiany kodu, w tym szczegółów hacków. Handlowymi odpowiednikami Usenetu były sieci o wartości dodanej (VAN), takie jak America On Line (AOL), CompuServe i Prodigy. Te usługi są świadczone przez modemy do dostępu telefonicznego, poczty elektronicznej i urządzeń do definiowania grup dyskusyjnych. Opłaty wahały się od godzinowych do miesięcznych.

połowa lat 1990: łączne połączenia międzysystemowe. Wraz z rosnącą popularnością sieci LAN pojawiły się technologie ich łączenia. Te sieci fizycznie połączonych sieci lokalnych nazywa się sieciami rozległymi (WAN). Każdy węzeł w sieci LAN może uzyskać dostęp do każdego węzła w dowolnej innej połączonej sieci LAN, a w niektórych konfiguracjach te węzły mogą również uzyskać dostęp do plików typu mainframe i minikomputerów oraz do możliwości przetwarzania.

Telepraca: Po uruchomieniu technologii WAN stało się możliwe łączenie sieci LAN za pomocą obwodów telekomunikacyjnych. Było to drogie w porównaniu z niskobudżetowymi systemami online lat 70., ponieważ wszystkie dane musiały być przesyłane przez sieć. Ponieważ przetwarzanie i większość danych używanych przez stację roboczą znajdowały się w lokalnej sieci LAN, sieć WAN była znacznie tańsza. Łącza LAN zostały połączone za pomocą dostępu dial-up w celu zminimalizowania kosztów, podczas gdy główne sieci LAN zostały połączone z dedykowanymi obwodami o wysokiej prędkości w celu zwiększenia wydajności. Oprócz dostępu dial-up cały ruch sieciowy zazwyczaj przepływa przez niedzwonione sieci prywatne. Spośród tych dwóch metod komunikacja dial-up była znacznie bardziej podatna na naruszenia bezpieczeństwa i pozostają one do dziś.

Internet i sieć WWW : Internet, który rozpoczął życie w 1969 roku jako Sieć Agencji Zaawansowanych Projektów Badawczych (ARPANET), powoli pojawił się na ogólnej scenie komputerowej w latach osiemdziesiątych. Początkowo dostęp do Internetu był ograniczony do agencji rządowych USA i ich kontrahentów. Użytkownicy ARPANET wprowadzili koncepcję poczty elektronicznej jako wygodny sposób komunikacji i wymiany dokumentów. Następnie w latach 1989-1990 Sir Tim Berners-Lee wymyślił World Wide Web i przeglądarkę internetową. Ta jedna koncepcja spowodowała głęboką zmianę w Internecie, znacznie zwiększając jej użyteczność i tworząc nieodparty popyt na dostęp. W latach 90. rząd USA zrezygnował ze swojej kontroli, a Internet stał się gigantyczną, niezależną siecią sieci, jaką jest dzisiaj. Wybuchowy wzrost udziału w globalnym Internecie jest ogólnie postrzegany jako rozpoczynający się od otwarcia domeny najwyższego poziomu .COM do powszechnego użytku w 1993 roku. Internet oferuje kilka ważnych zalet: Koszt jest stosunkowo niski, połączenia są dostępne lokalnie w większości krajów uprzemysłowionych i poprzez przyjęcie protokołu internetowego, TCP / IP, każdy komputer staje się natychmiast kompatybilny z wszystkimi innymi użytkownikami Internetu. Technologia sieci WWW ułatwiła każdemu dostęp do zdalnych danych. Niemal z dnia na dzień Internet stał się kluczem do globalnej sieci. Dostawcy usług internetowych (ISP) obsługują komputery zgodne z Internetem zarówno z dostępem dial-up, jak i dedykowanym. Komputer może uzyskać dostęp do usługodawcy internetowego bezpośrednio jako autonomiczny klient ISP lub przez bramkę z sieci LAN

lub WAN. Duży dostawca usług internetowych może oferować dostęp dial-up w wielu lokalizacjach, czasem nazywanych punktami obecności lub POP, połączonymi przez własną sieć. Dostawcy usług internetowych tworzą powiązania między sobą za pośrednictwem krajowych punktów dostępu (NAP), początkowo utworzonych przez National Science Foundation. Dzięki temu "kręgosłupowi" każdy węzeł z dostępem może komunikować się z innym węzłem, połączonym z innym dostawcą usług internetowych, zlokalizowanym w połowie globu, bez wcześniejszych ustaleń. Nieograniczony dostęp zapewniony przez Internet stwarza nowe możliwości dla organizacji do komunikowania się z klientami. Firma może wdrożyć serwer sieciowy z pełnym połączeniem z usługodawcą internetowym i udostępnić publicznie serwer WWW i strony WWW, które udostępnia. Potencjalny klient może uzyskać dostęp do Witryny, pobierać informacje o produktach i aktualizacje oprogramowania, zadawać pytania, a nawet zamawiać produkty. Strony komercyjne, ponieważ ewoluowały ze statycznych "prospektów" do centrów handlowych online, domów maklerskich i biur podróży, aby wymienić tylko kilka z nich, stały się znane jako e-biznes.

Wirtualizacja i chmura: Już pod koniec lat 60. udostępniono oprogramowanie do tworzenia zamkniętych wersji systemu operacyjnego na komputerach typu mainframe. Użytkownicy wchodzili w interakcję z tym, co wyglądało na własne, prywatne środowisko mainframe. Pod koniec lat 80. dostawcy stworzyli symulacje środowisk operacyjnych, które mogą działać w różnych systemach operacyjnych (np. Można uruchamiać programy DOS na komputerach z systemem UNIX). Trend utrzymywał się przez kolejne lata, więc obecnie powszechne jest uruchamianie programów pod hiperwizorami, które symulują pełne lub funkcjonalnie ograniczone wersje wymaganych systemów operacyjnych na współdzielonym sprzęcie. W dzisiejszych czasach możliwe jest dostarczanie użytkownikom wystąpień środowiska operacyjnego na współdzielonym sprzęcie, często na odległość, dzięki czemu przyrost wymagań może zostać osiągnięty przy niewielkich kosztach, zamiast konieczności zakupu udoskonalenia na dużą skalę infrastruktury sprzętowej. Sytuacja jest podobna do tego, co oferowane przez biura usług w dziesięcioleciach, gdy dzielenie czasu na mainframe było popularne. Kolejną zmianą w ostatnim dziesięcioleciu była dostępność chmury obliczeniowej, która odnosi się do usług komputerowych, w tym pamięci masowej, oprogramowania jako usługi (SAAS) oraz infrastruktury lub platformy jako usługi (IAAS i PAAS).

KONTROLA NADZORU I POZYSKIWANIA DANYCH

Wykorzystanie komputerów do kontrolowania produkcji towarów i usług za pomocą oprogramowania i sprzętu do kontroli nadzorczej i pozyskiwania danych (SCADA) rosło przez cztery dekady od czasu opublikowania tego podręcznika w 1973 r. Systemy SCADA dla infrastruktury krytycznej były bardzo niepokojące, ponieważ w przeciwieństwie do początkowych specyfikacji projektu, wiele z nich zostało połączonych z ogólnym Internetem, otwierając systemy, którymi rządzą, na subwersję.